

Letter Report

Classification Approach for Digital I&C Systems at U.S. Nuclear Power Plants

R. T. Wood, R. A. Joseph III, K. Korsah, M. D. Muhlheim, J. A. Mullens
Oak Ridge National Laboratory

Project Manager: T. Burton, NRC RES
Principal Investigator: R. T. Wood, ORNL

February 2012

Prepared for the
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6165
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

Page intentionally blank

CONTENTS

	Page
LIST OF FIGURES	v
LIST OF TABLES	vii
GLOSSARY	ix
1. INTRODUCTION	1
1.1 Objectives of Research for Developing Classification Approach	1
1.2 Research Approach	2
1.3 About This Report	2
2. INVESTIGATION OF APPROACHES TO CLASSIFICATION	3
2.1 Safety Significance	3
2.2 Physical Representation	6
2.3 Functional Representation	10
2.4 Critical Characteristics	14
2.5 Conclusions	18
3. CLASSIFICATION STRUCTURE	21
3.1 System Class	22
3.2 Function Class	24
3.3 Platform Class	27
3.3.1 Investigation of available platform information	27
3.3.2 Attribute Categories for the Platform Class	28
4. CLASSIFICATION STRUCTURE APPLIED TO THE DI&C INVENTORY	33
4.1 System Class Structure and Associations	33
4.2 Decomposition of System Class	34
4.3 Function Class Structure and Associations	34
4.4 Linking System and Function Classes	36
4.5 Platform Class Structure and Associations	36
4.6 Linking System and Platform Classes	37
4.7 Linking Platform and Function Classes	40
4.8 Fully Integrated DI&C Classification Structure	40
5. CONCLUSIONS	43
6. REFERENCES	45
APPENDIX A. GENERIC SYSTEMS FOR BWR AND PWR DESIGNS	A-1
APPENDIX B. PLANT FUNCTIONS FOR A PWR DESIGN	B-1
APPENDIX C. ATTRIBUTE CATEGORIES FOR THE INFORMATION STRUCTURE OF THE PLATFORM CLASS	C-1

Page intentionally blank

LIST OF FIGURES

Figure	Page
1	Block diagram of main elements of an instrument channel..... 6
2	Whole-part representation of a system. 7
3	Subsystem representation of an I&C and HSI system. 7
4	Block diagram of a typical I&C function for an instrument channel. 10
5	Beltracchi analysis framework. 12
6	Conceptual classification of DI&C systems. 18
7	Structural representation of system architecture..... 23
8	Expansion of block representation to illustrate presentation of greater detail..... 24
9	High-level functional–physical representation of a plant function..... 26
10	DI&C inventory data objects for the system class..... 33
11	Hierarchical data decomposition within the system class. 34
12	DI&C inventory data objects for the function class. 35
13	Data association between system and function classes. 36
14	DI&C inventory data sets and data object for the platform class. 37
15	Data association between system and platform classes. 38
16	Extended data associations between system and platform classes. 39
17	Simplified decomposition illustrating relationship between system and platform classes..... 39
18	Elementary data association between function and platform classes. 40
19	Overall classification structure for DI&C inventory. 41

Page intentionally blank

LIST OF TABLES

Table		Page
1	Comparison of international safety classification structures	5
A.1	Catalog of generic systems for a BWR design	A-3
A.2	Catalog of generic systems for a PWR design.....	A-4
B.1	Catalog of plant functions for a PWR design	B-3
C.1	Attribute categories for the information structure of the platform class.....	C-3

Page intentionally blank

GLOSSARY

architecture	<p>The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment. [IEC 42010]</p> <p>The organizational structure of a system or component. [IEEE 100]</p> <p><i>Note:</i> A plant I&C architecture is the organizational structure of the I&C systems of the plant. [IEC 61513]</p>
characteristic	<p>Any property or attribute of an item, process, or service that is distinct, describable, or measurable. [IEEE 100]</p> <p>A feature or quality that makes something recognizable.</p>
class	<p>A category into which objects are placed on the basis of both their purpose and their internal structure. [IEEE 100]</p>
classification	<p>A systematic arrangement into classes or groups. The allocation of items to groups according to type (e.g., on the basis of identified characteristics).</p>
component	<p>A part or assembly of parts that is viewed as an entity for purposes of design, operation, and reporting. One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components. <i>Note:</i> The terms “module,” “component,” and “unit” are often used interchangeably or defined to be subelements of one another in different ways depending upon the context. [IEEE 100]</p>
decomposition	<p>Separation or disassembly into constituent parts (e.g., components, functions). <i>Note:</i> Hierarchical decomposition is a form of modular decomposition in which a system is broken down into a hierarchy of components through a series of top-down refinements.</p>
equipment	<p>An assembly of components designed and manufactured to perform specific functions. <i>Note:</i> Examples of equipment are motors, transformers, valve operators, and instrumentation and control devices. [IEEE 100]</p>
function	<p>A defined objective or characteristic action of a system or component. For example, an I&C system may have inventory control as its primary function. [IEEE 100]</p> <p><i>Note:</i> A plant function is an I&C function to control, operate, and/or monitor a defined part of a process. An I&C function may be subdivided into a number of subfunctions (for example, measuring function, control function, actuation function) for the purpose of allocation to I&C systems. [IEC 61513]</p>
functionality	<p>The capabilities of the various computational, user interface, input, output, data management, and other features provided by a digital product (i.e., platform). [IEEE 100]</p>
functional element	<p>An entity of hardware, software, or both capable of accomplishing a specified purpose. [IEEE 100]</p>
module	<p>Any assembly of interconnected components that constitutes an identifiable device, instrument, or piece of equipment. [IEEE 603]</p>

plant I&C architecture	Organizational structure of the I&C systems of the plant. [IEC 61513]
platform	Any base of technologies on which other technologies, processes, or systems are built. For example, a computer-based platform is an underlying computer system on which application programs can be executed. For digital I&C systems, a platform is the digital equipment (e.g., device, base product line) that is implemented (i.e., designed, programmed, configured, installed) as the basis for a system to accomplish plant functions. The platform provides fundamental capabilities for instantiating functions as digital applications.
system	<p>A collection of several components, assembled in such a way as to perform a specific (active) function. A component is a discrete element of a system. [IAEA Safety Guide]</p> <p>A set of elements that interact according to a design, where an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction. [IEC 61508]</p> <p>A combination of two or more interrelated components that perform a specific function related to plant operation and safety. A system may perform a function such as control, monitoring, electrical, mechanical, or structural. [IEEE 100]</p> <p><i>Note:</i> An I&C system, based on electrical and/or electronic and/or programmable electronic technology, performs I&C functions as well as service and monitoring functions related to the operation of the system itself. The general use of the term encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices. [IEC 61513]</p> <p><i>Note:</i> A digital I&C system is a digital implementation of an I&C system at a plant.</p>
system architecture	The structure and relationship among the components of a system. The system architecture may also include the system's interface with its operational environment. [IEEE 100]
system element	<p>One or more software, hardware, or firmware components that perform a specified task.</p> <p><i>Note:</i> A system element may be composed of a combination of system elements. [IEEE 100]</p>

Classification Approach for Digital I&C Systems at U.S. Nuclear Power Plants

LETTER REPORT

R. T. Wood, R. A. Joseph III, K. Korsah, M. D. Muhlheim, J. A. Mullens
Oak Ridge National Laboratory

February 2012

1. INTRODUCTION

Instrumentation and control (I&C) systems are vital to nuclear power plant operation and safety. Specifically, I&C systems provide operators with critical plant information and automatically command the nuclear and process systems at a plant to maintain control and ensure safety. In recent years, nuclear facilities have undertaken modernization projects to address obsolescence of their analog-based safety-related systems and equipment through implementation of digital replacements. The transition to digital I&C (DI&C) systems in safety-related applications at nuclear power plants (NPPs) poses the challenge of addressing new failure modes, including the potential for common-cause failure vulnerability, that arise from unique characteristics of digital technology. Key elements to resolving this challenge involve (1) establishing the context for safety-related usage of digital technology and (2) developing an approach to enable determination of commonalities in performance and failure modes of DI&C systems. The first element implies the need for an inventory to characterize the extent to which DI&C systems have been implemented at NPPs in the United States. The second element suggests the need for a means to organize experience data and technical information about DI&C systems into related classes based on key features, characteristics, and behavior.

1.1 Objectives of Research for Developing Classification Approach

The U.S. Nuclear Regulatory Commission (NRC) Office of Nuclear Regulatory Research (RES) engaged the Oak Ridge National Laboratory to initiate an inventory of DI&C systems in domestic NPPs and develop the basis for an approach to classifying those systems. The inventory data and classification structure that are the principal products of the two main research tasks are intended to facilitate the review and evaluation of technology usage and operating experience (OpE) data. The objective of this research element of the project is to establish a classification structure that can be applied to data from an inventory of DI&C systems to enable enhanced knowledge extraction from the information gathered. To fulfill project expectations, the classification approach must (1) meet NRC system analysis needs, (2) provide a suitable structure for organizing the inventory information, and (3) be sufficiently flexible to support the subsequent introduction of expanded information categories and additional data as the DI&C inventory evolves.

The classification of DI&C systems provides a means by which information on the use of digital technology can be categorized in terms of key characteristics. Definition of a classification scheme for DI&C systems can help establish relevance of OpE among different applications. In addition, a classification structure can provide the basis for determining commonalities among different DI&C systems, platforms, or implementation approaches to (1) focus proper attention on key vulnerabilities and (2) recognize technological strengths and effective practices.

In addition to physical or logical elements of DI&C systems, characteristics or features of those systems, such as technology, architecture, function, performance, robustness, and dependability, can serve as

categories within a classification structure. These characteristics can provide the basis for establishing relational attributes of those systems to enable aggregation of information and support the identification and evaluation of any unique safety issues posed by the digital technology. However, the classification structure must be relevant to the information that is available for collection. The development of the initial DI&C inventory is described in a companion letter report.¹ The fundamental information captured to form the basis for the inventory consists of the identification of the digital system (e.g., supplier, platform, product identification, etc.) and its application (i.e., plant I&C system) by unit at each NPP. Therefore, the classification structure must be founded on these central information items.

The principal global data of the inventory (i.e., system and platform by plant) represents a first cut at information gathering. Thus, it is recognized that additional data may become available as more detailed plant-specific information (e.g., architecture, interconnections, locations, environments) or platform-specific information (e.g., hardware configuration, platform capabilities, software usage, life cycle processes) is acquired. Therefore, the classification structure must provide sufficient flexibility to address the range of information that may become available and also offer acceptable expandability to accommodate new data categories that may arise.

1.2 Research Approach

The research approach employed in this activity involved an investigation of classification approaches documented in available publications, reports, and information sources to identify relevant schemes for consideration. The identified classification approaches were then evaluated to determine their suitability for using directly with or adapting the approach to an inventory of DI&C systems at domestic NPPs. Based on the findings of that assessment, a classification structure was devised, and a concept for its application to the baseline DI&C inventory was developed.

1.3 About This Report

This report presents the findings of the investigation of classification approaches and documents recommendations for a classification structure. More specifically, Sect. 2 summarizes each of four approaches identified from the literature that could serve as methodologies for classifying I&C systems and provides observations about aspects of each approach that were considered relevant or useful in meeting one or more of the three objectives noted in Sect. 1.1. Section 3 discusses the three classes of information (system, function, and platform), their respective attributes that form the structure of the recommended classification approach, and the processes for further decomposing or subdividing information (design aspects, implementation approaches, functionality, etc.) into more refined data elements, thereby accommodating more detailed information about the I&C system. In Sect. 4, the recommended classification approach is discussed as applied to the DI&C inventory that is being developed.¹ The structure and data elements for each of the three information classes are presented along with identification of the important associations that relate these three classes and, thus, define the overall classification framework. Section 5 summarizes this research noting that the recommended classification structure developed herein provides a framework and structure for establishing the initial set of key relationships among the three classes—system, function, and platform—that not only supports the “characterization” of DI&C systems but also provides the foundation for later development of a relational database and/or information system to readily search detailed information on DI&C systems.

2. INVESTIGATION OF APPROACHES TO CLASSIFICATION

Available publications, reports, and information sources were investigated to determine if a classification framework suitable for characterizing DI&C systems could be identified. The investigation considered classification and system representation schemes from nuclear power applications as well as approaches from relevant technical domains such as digital technology, systems analysis, and cognitive engineering. The identified classification approaches can be characterized in terms of four primary types based on the means of organizing information. These approaches to representing system information are:

- safety significance,
- physical representation,
- functional representation, and
- critical characteristics.

This section summarizes the identified classification approaches that were evaluated further to determine their suitability to serve as the basis for a classification framework. No specific classification framework was found that fully satisfies the objectives noted in Sect. 1.1. However, key aspects or qualities of several approaches were identified that can be adapted into recommendations for a classification structure that can be employed to organize DI&C inventory information and support analyses of failure modes, performance, or safety characteristics from OpE data. These observations of suitable features are noted in the discussions that follow.

2.1 Safety Significance

The nuclear power industry has historically classified I&C systems according to safety significance. This classification approach is based on a deterministic assessment of the role in assuring safety that is assigned to the functions accomplished by those systems. Safety classification is well established, and the scope of this project does not involve replacement or modification of the current structure. Nevertheless, safety significance is a key characteristic of I&C systems at NPPs, and there are notable variations within international safety classification structures. Therefore, this section gives an overview of the prevailing safety classification approaches employed by the international nuclear power industry.

Title 10, Part 50 of the Code of Federal Regulations (CFR)² establishes a classification approach for structures, systems, and components (SSCs) in a nuclear power facility. Section 2 of 10 CFR 50 defines safety-related SSCs in terms of reliance on those SSCs to remain functional during and after design basis events to assure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain a safe shutdown condition, and (3) the capability to prevent or mitigate the consequence of accidents that could result in unacceptable offsite exposures.

For electrical and I&C equipment, 10 CFR 50.49 identifies classification of systems as important to safety. The scope of systems included in the important-to-safety class include safety-related systems, those nonsafety-related systems whose failure under postulated environmental conditions could prevent satisfactory accomplishment of safety functions by safety-related systems, and certain post-accident monitoring systems.

The Institute of Electrical and Electronic Engineers (IEEE) further identifies I&C systems that are important to safety as Class 1E equipment. In IEEE standard (Std) 323-2003 [Ref. 3], Class 1E is defined as the “safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.”

In addition to the traditional deterministic classification approach, a risk-informed approach to safety classification has been established in 10 CFR 50.69. Specifically, SSCs are divided into risk-informed safety classes based on both deterministic safety classification and probabilistic significance to plant safety. In this classification approach, insight from a probabilistic risk assessment (PRA) on the safety significance of the function performed by a system is captured based on its contribution toward reducing the risk of release of radioactive material to the environment. A safety-significant function is defined as “a function whose degradation or loss could result in a significant adverse effect on defense-in-depth, safety margin, or risk.” The four risk-informed safety classes (RSICs) are defined as follows:

- **RISC-1** includes safety-related systems that perform safety significant functions,
- **RISC-2** includes nonsafety-related systems that perform safety significant functions,
- **RISC-3** includes safety-related systems that perform low safety significant functions, and
- **RISC-4** includes nonsafety-related systems that perform low safety significant functions.

The International Atomic Energy Agency (IAEA) defines a deterministic safety classification for I&C systems in IAEA Safety Guide NS-G-1.3 [Ref. 4]. The classification approach involves assigning a safety class based on the importance to safety of the function performed by the I&C system. Thus, the safety guide divides I&C systems into “systems important to safety” and “systems not important to safety.” An I&C system important to safety is one whose malfunction or failure could lead to unacceptable radiation exposure of the site personnel or members of the public. Systems important to safety are further subdivided into “safety systems” and “safety-related systems.” Safety systems perform protective functions while safety-related systems are those I&C systems that perform important functions other than the main protective functions.

The standards issued by the International Electrotechnical Commission (IEC) adhere to the safety principles established by the IAEA. However, the IEC refines the safety classification approach established by the IAEA by resolving the important to safety class based on a three-tiered approach to identifying both I&C systems and the functions they perform. The IEC safety classification approach is based on the IAEA safety philosophy and the plant design base. All SSCs that are items important to safety, including software for digital I&C systems, are classified on the basis of their function and significance with regard to safety. Basically, I&C systems that provide functions to cope with postulated initiating events (PIEs) are classed in the highest safety class while less important functions and equipment are assigned to lower safety classes.

IEC standards provide criteria for assignment of functions to safety categories and establish design requirements for the corresponding I&C systems and equipment. In IEC 61513 [Ref. 5], the general requirements for I&C systems important to safety are established in terms of safety classes. I&C systems are assigned to one of three safety classes (Class 1, Class 2, and Class 3), or are unclassified, based on their main safety function. The determination of classification for safety functions is established in IEC 61226 [Ref. 6]. This standard classifies functions into three categories (Category A, Category B, Category C). Category A corresponds to functions that play a principal role in the achieving or maintaining safety by preventing design basis events from leading to unacceptable consequences. Category B covers functions that play a complementary role to the Category A functions in assuring safety, especially those functions that are required to operate after a nonhazardous stable state has been achieved. Category B also includes functions whose failure could initiate a design basis event or worsen the severity of an event. Category C addresses functions that play an auxiliary or indirect role in the achievement or maintenance of NPP safety. Other functions that do not meet the criteria of the three categories are identified as “nonclassified” (NC).

In addition to the international classification approach defined in safety guides and standards, various national approaches exist that reflect domestic practice and conventions. Table 1, which was adapted from Ref. 7, illustrates several safety classification approaches that have been reviewed. The table does not

constitute a high-fidelity mapping of the classes and categories employed by the international nuclear power industry but, rather, it is intended to provide a general indication of the approximate relationship among the classification approaches.

The safety classification approaches that were investigated generally involve a deterministic assessment of the safety significance of the main function performed by an I&C system. As seen in the establishment of the RISC classes, risk insights can be incorporated into the safety classification structure. While revision of well-established safety classification practices is not within the scope of this research, it is a fundamental requirement that any classification approach developed for treating DI&C system information must be compatible with and complementary to the existing safety classes. In effect, the DI&C inventory must be capable of representing the safety significance of each DI&C system as established by the safety classification approaches identified above. This objective can be accomplished by incorporating a safety class (or category) identifier as a data element associated with each implemented system captured in the DI&C inventory.

Table 1. Comparison of international safety classification structures

National or international standard	Classification of the importance to safety			
USA	Systems important to safety			Nonsafety
	Class 1E, safety, or safety-related	Systems whose failure can inhibit safety functions		
	RISC-1, RISC-3			RISC-2, RISC-4
IAEA	Systems important to safety			Systems not important to safety
	Safety	Safety related		
IEC 61226	Systems important to safety			Unclassified
	Category A	Category B	Category C	
IEC 61513	Systems important to safety			Unclassified
	Class 1	Class 2	Class 3	
European Utility Requirements	F1A (automatic)	F1B (automatic and manual)	F2	Unclassified
France N4	1E	2E	IFC/NC	
Japan ^a	PS1/MS1	PS2/MS2	PS3/MS3	Nonnuclear safety
Korea	IC-1	IC-2	IC-3	Non-IC
Russia	Class 2 (safety system, design basis accident)	Class 3		Class 4 (systems not important to safety)
Switzerland	Category A	Category B	Category C	Not important to safety
UK	Category 1		Category 2	Unclassified

^aPS = prevention system, MS = mitigation system

2.2 Physical Representation

Information on I&C systems can be most directly captured and organized in terms of the physical elements of the implemented system. Block diagrams and schematics provide an amenable structure with which to provide an abstract representation of the more detailed physical layout of a system, module, or circuit. For example, Fig. 1 shows a physical representation of a typical NPP instrument channel from sensor to actuator. A physical representation is an especially convenient approach to capture information on analog I&C systems, in which discrete elements typically provide dedicated, hardwired functionality. For DI&C systems, multiple functions can be realized in a single module via software implementation, and the complexity of the computational element makes it difficult to isolate specific functions or capabilities. Consequently, it is more difficult to represent a DI&C system solely by a physical model.

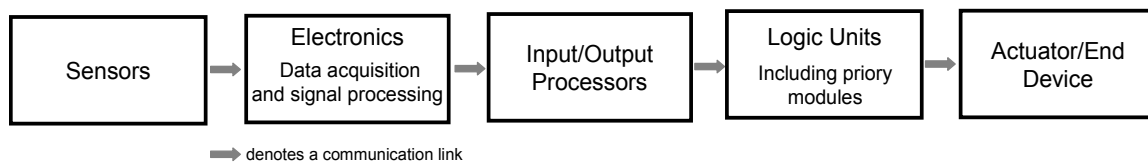


Fig. 1. Block diagram of main elements of an instrument channel.

Nevertheless, a physical representation of a plant I&C architecture, system, subsystem, module, or component provides a direct link with actual implementation of I&C systems within an NPP. Detailed element-by-element capture of information given the large number of constituent physical components in an overall plant I&C architecture is an imposing task. Thus, an abstraction of the physical implementations of the many DI&C systems is necessary to enable inventory data to be practically captured and collated. A common practice to manage complexity is to employ a *whole-part* abstraction to represent the physical architecture. In a whole-part abstraction, a system is modeled as a group of related components at several levels of physical aggregation. Effectively, the approach establishes a hierarchical decomposition of higher-level physical systems into subelements in which the relationship of parts to the whole is represented. Figure 2 illustrates a whole-part abstraction approach applied to a generic system.

Adopting a physical representation approach to classification begins with identification of the I&C systems that constitute the overall plant I&C architecture. An example of a whole-part abstraction of I&C systems within the nuclear power industry is found in the technology roadmap on instrumentation, control, and human-machine interface to support the U.S. Department of Energy Advanced Reactor programs.⁸ Specifically, the roadmap characterized a generic I&C and human-system interface (HSI) system in terms of subsystems involving sensors, monitoring, automation and control, communication, and human-system interfaces.

This model for representing a system was expanded and used to establish a framework to support classification of I&C system degradation as part of a study by Brookhaven National Laboratory (BNL) on the impact of such degradation on human performance.⁹ In the BNL framework, the HSI subsystem was decomposed to consist of six subsystems:

- alarms,
- information systems,
- computerized operator support systems (COSSs),
- controls,
- communication systems, and
- workstations.

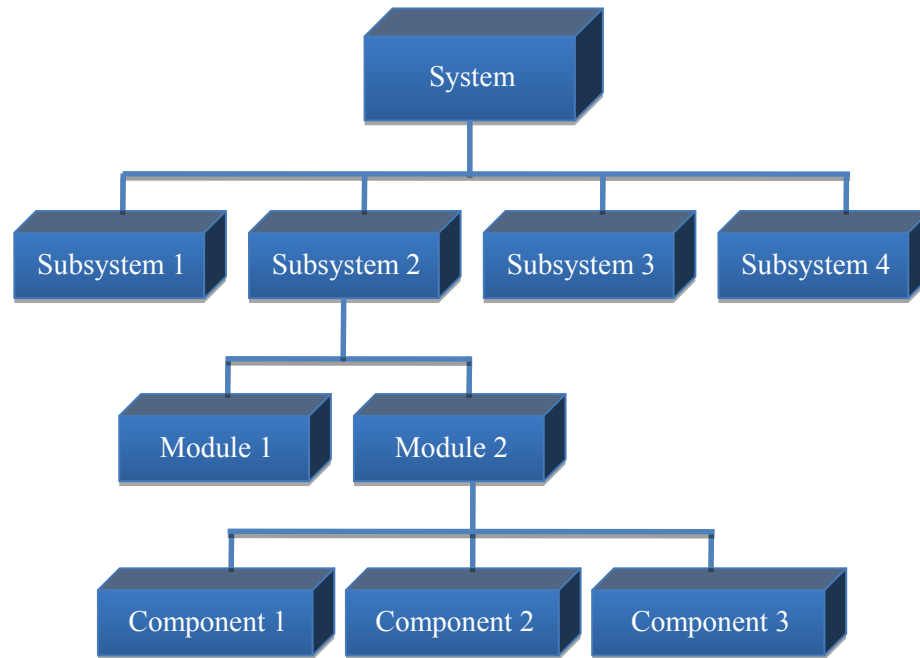


Fig. 2. Whole-part representation of a system.

By coupling the physical representation of an I&C and HSI system to human performance factors, the BNL study established a framework to support top-down and bottom-up analyses of the impact of I&C degradation on operator tasks. The interrelationships established between I&C subsystems, HSI subsystems, and functional tasks corresponding to key human performance factors are shown in Fig. 3. Although examples are documented in the report, the comprehensive set of direct associations between the levels of the framework remains to be developed through detailed system and task analyses.

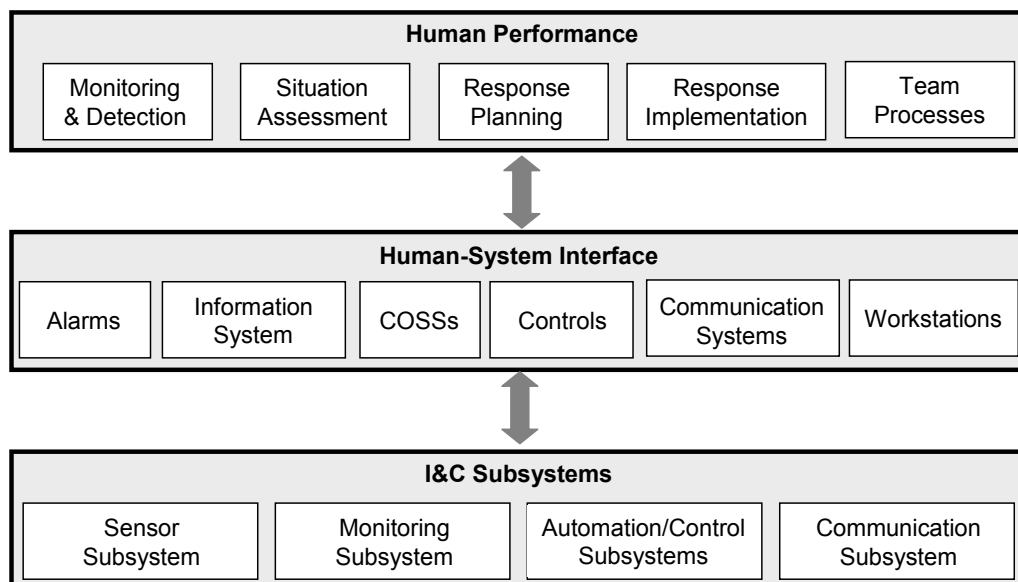


Fig. 3. Subsystem representation of an I&C and HSI system.

This classification approach is intended to provide a framework for analysis rather than an inventory structure. However, it does indicate organization and data linkage considerations that can be adapted in the development of a DI&C inventory. In particular, this framework model demonstrates how human interaction elements of DI&C systems can be incorporated into a physical representation. In addition, an approach to linking key characteristics of an application, human performance in this case, with an architectural representation of systems as a means to support analyses is also identified. The key to adopting this approach is to establish the linkage or association between system elements and characteristics of interest (e.g., performance, design, failure).

An example of a database within the nuclear power industry that utilizes a physical representation of plant systems to contribute to the organization of data is found in the coder's manual for the Sequence Coding and Search System (SCSS).¹⁰ The SCSS provides a searchable database of licensee event reports (LERs). As part of the SCSS, system codes are provided for types of I&C systems. There are 18 codes identified in the coder's manual. These system categories identified for the SCSS are the following:

- alarms/annunciators,
- (plant) computer,
- fire detection,
- environmental monitoring,
- emergency generator I&C,
- turbogenerator I&C,
- plant monitoring/post-accident monitoring,
- in-core/ex-core neutron monitoring,
- pressure boundary leak monitoring,
- radiation monitoring,
- reactor power control,
- recirculation flow control,
- feedwater control,
- reactor protection,
- engineered safety features actuation,
- solid state protection and control system,
- anticipated transient without scram, and
- nonnuclear instrumentation.

Within the SCSS structure, a system can be further identified through a manufacturer's code, an interface code (identifying those plant systems to which the specific system has an interface), and a code identifying the type of component involved in the initiation of the reportable event. However, the categorization of systems for the SCSS does not serve as the basis for its primary classification of data. The event is the fundamental data object in the classification approach employed for the SCSS rather than the system or component. In particular, codes are provided characterize the event and its consequences. These codes include proximate cause, effect on plant, shutdown method, facility status, method of discovery/detection, form and content of any activity release, and type of personnel exposure. Thus, while the SCSS employs a high-level physical representation of plant systems in extracting data from LERs, the physical instance of a system or component is captured as a data attribute corresponding to an event rather than primary data object of interest, as would be the case in an inventory. Nevertheless, the coupling of system data with event data illustrates a means of linking or associating data collections of one type (e.g.,

an inventory) with data collections of another type (e.g., event or failure databases) through common data items (i.e., attributes or properties for data objects).

Two other DI&C system information collections that involved physical representations in collating data were identified in the investigation of classification approaches. In one case, the Electric Power Research Institute (EPRI) project to develop qualification guidelines for application of programmable logic controllers at NPPs^{11,12} included an effort to generate technical descriptions for I&C systems at NPPs. The information capture involved identification of safety-related and nonsafety-related I&C systems at NPPs (see Appendix A). In addition, the systems were decomposed according to five attributes: system architecture, input signals, output signals, operator interface, and system functions. The first four attributes primarily correspond to physical elements of the I&C system. However, the fifth attribute involves a functional representation of the system. In addition, the physical attributes also include subattributes that arise from critical characteristics such as modes of operation, testability and self-diagnosis, access control, and so forth. The system identification provided by the EPRI reports is suitable for incorporation into the basis for a classification structure to support a DI&C inventory. However, the decomposition of I&C systems presented in the reports is very dated, based on an early-1990s architectural context, so the detailed structure would need updating to be directly useful. Nevertheless, the association of physical, functional, and critical characteristic attributes within a comprehensive structure suggests an approach that can be adapted to capture the necessary information about DI&C systems to support flexible analysis of OpE information.

In the other case, EPRI TR-1001503 (Ref. 13) documents an effort from the late 1990s to capture digital platform information from system vendors. The objective of that research was to develop a database containing detailed technical descriptions of DI&C systems and components. The approach involved a survey of vendors. A database application involving three databases was populated based on the results of the survey. The databases consisted of a “Vendors” database containing vendor information, a “Systems” database capturing the capabilities of the product line, and a “Utilities” database containing data about specific implementations of a platform at NPPs. The systems and their implementations were represented based on a hierarchical structure or data “tree.” The database application was not maintained and is no longer available. However, the report indicates the structure and categories of its content. The basic architecture of a system (i.e., components and configuration) was recorded, along with design features. Functionality was represented in terms of coverage of functional types, configurability and flexibility. Characteristics addressing performance (e.g., capacity, response time, accuracy) and dependability (e.g., integrity, reliability, maintainability, security) were also included. In addition, other information such as software principles applied, training offered, technological options, and standards employed were captured. Information about the implementation project was also identified, including as system requirements, classification, project development, quality assurance, etc. The approach used for this database illustrates how a physical representation of a system (in this case, a digital platform) can be combined within implementation and supplier specific information in a multiclass data structure to organize critical characteristics, architectural features, and functional capabilities in a searchable framework. Aspects of this approach are suitable for incorporation as the basis for flexible classification structure to support generation of a comprehensive DI&C inventory that can support system and OpE analyses.

Several observations can be drawn regarding classification approaches based on physical representations. First, the prior reported inventory efforts have not resulted in lasting resources nor defined a comprehensive DI&C classification structure. Second, a physical representation provides a basis for organizing information about DI&C systems that can be readily associated with the actual implementations and specific configurations, thus preserving a relationship with the installed I&C systems. In particular, a whole-part abstraction approach permits I&C system architectures to be represented while supporting capture of more detailed configuration information through successive decompositions through the whole-part hierarchy. Third, features and capabilities, such as software and

human interfaces, strongly depend on recognition of function and critical characteristics that cannot be completely represented solely on the basis of a physical model. Thus, a classification structure that enables physical, functional, and critical characteristic information to be captured and interrelated seems likely to serve as a suitable framework for a DI&C inventory to support OpE and other system analyses.

2.3 Functional Representation

As discussed in Sect. 2.1, function relates to purpose and serves as a primary basis for the establishment of safety classification. A functional representation of I&C systems is frequently illustrated in block diagram form with the primary functions that are assigned to different elements of a system identified as blocks arranged to correspond with architectural (i.e., physical) structure of the I&C system. A functional block diagram that is comparable to the instrument channel diagram of Fig. 1 is shown in Fig. 4. The unidirectional arrows represent data flow while the bidirectional arrow indicates the functional interconnections between the channel functions and the interface functions for human interaction.

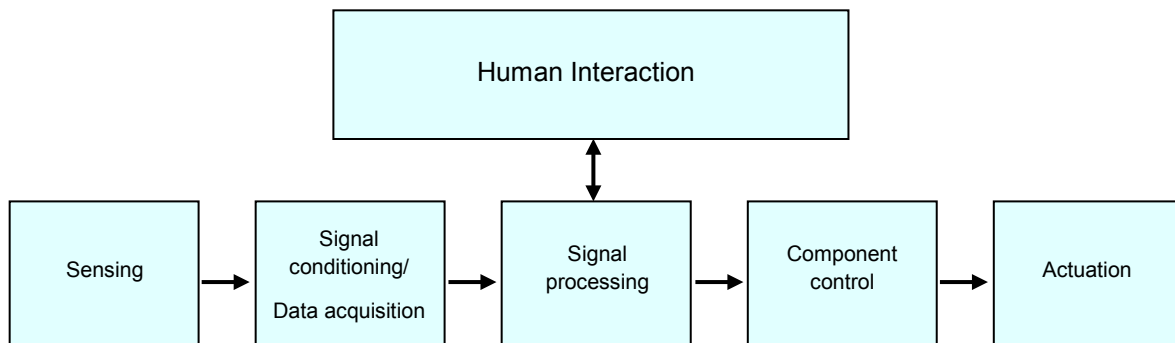


Fig. 4. Block diagram of a typical I&C function for an instrument channel.

As part of a reference report on I&C systems in NPPs, the IAEA provides a basic introductory description of I&C systems.⁷ The report notes that the variety of technological elements that constitute the I&C system architecture of an NPP can be difficult to address as a whole because of the depth and breadth of the discipline. Consequently, the report characterizes the I&C systems in terms of three viewpoints, which facilitate a representation of the full scope of the technical discipline. The viewpoints are identified as functional, physical, and lifecycle. It is noted that these viewpoints for representing the I&C systems of an NPP serve to illustrate the purpose of the I&C systems (functional), the embodiment of those systems (physical), and the means by which those systems are realized and maintained (lifecycle).

The functional approach employed in the IAEA report to characterize a generic I&C system architecture focuses on plant-wide system objectives and the means of achieving those objectives. Specifically, the report presents a function-based representation that addresses the sensory, communications, monitoring, display, control, and command systems interposed between the process (i.e., the reactor, heat transport, and energy conversion systems), and the plant personnel (i.e., operations and maintenance staff). A whole-part decomposition of function, from plant function to system functionality, is illustrated through basic examples and a high-level overview of a generic functional architecture. The functional architecture representation adopts a coupled functional–physical approach in which the distribution of function within the I&C architecture of a plant is addressed at a high level of aggregation. The representation described in the IAEA report is conceptual in nature and so it would need further development to be suitable as a basis for a classification approach for DI&C systems. Nevertheless, the concept of a coupling between functional and physical representations, with a hierarchical abstraction based on whole-part decomposition, can be incorporated into recommendations on organization structure for a DI&C inventory.

Within the field of cognitive systems engineering, Rasmussen¹⁴ established a functional abstraction hierarchy in which the structure embodies the relationship between goals and the method of accomplishing those goals (i.e., means to achieve an end). A means–ends abstraction hierarchy captures the functional properties of a system by relating ends (goals) at higher levels to means (methods) at lower levels. At each level of abstraction within the hierarchy, those functional properties are represented by distinct concepts such that each level describes the system in terms of a different set of attributes. Functional properties include information about the purpose of a system, the approach employed by a system (e.g., processes and phenomena), and the physical realization of a system. Thus, the organizational approach employed for capturing system function relates *what* (i.e., functional approach and modes of operation) at one level of the hierarchy to *how* (i.e., specific functions and functionalities) at the level below and *why* (i.e., goal) at the level above.

The conceptual framework established by Rasmussen involves the following levels of abstraction:

- functional purpose,
- abstract function,
- generalized function,
- physical function, and
- physical form.

At the highest level of abstraction, the overall purpose (i.e., the intended functional effect) of a system is represented. The abstract function level involves fundamental concepts and causal relationships to represent the overall proper function of a system. The generalized function level addresses basic functional relationships and natural processes that are independent of specific physical implementations. The functional states of a system, which are tightly related to its physical form, are represented at the physical function layer. Finally, the representation of physical form (i.e., components and configuration) provides the lowest, most concrete level of abstraction.

A top-down progression through the hierarchy establishes a “purpose” basis for the functional representation of a system to capture information on a specific purpose that can be realized by several physical implementations. A bottom-up progression through the hierarchy establishes a “physical” basis for the functional representation of a system to capture information on a specific implementation that can serve several purposes. The hierarchical structure associated with a means–ends abstraction suggests an approach to organizing functional information for I&C systems. The close connection between physical function and physical form at the lower levels of the hierarchy is consistent with common representations of function, as discussed above. In addition, the tie between purpose and functional implementation supports capturing the significance of functions. However, information necessary for the higher levels of abstraction is not readily available from likely sources for DI&C inventory data, so additional analysis would be required to populate the framework with information. Thus, adapting this structure directly for a DI&C inventory would not be straightforward.

Rasmussen et al.¹⁵ employed coupled means–ends abstraction and whole-part decomposition to establish a framework to support cognitive work analyses. The abstraction and decomposition hierarchies were applied to application areas or domains (e.g., the domain of potential risk and the domain of mitigation resources for analysis of decision making). In an unpublished white paper in 1995, Leo Beltracchi of NRC RES extended the Rasmussen analysis framework to address design and safety in the requirements for I&C systems at NPPs. In the Beltracchi approach, a means–ends abstraction hierarchy is applied to the domain of hazards and risk and the domain of mitigation and defense, which represent principle considerations in system design. The analysis framework also involves whole-part decomposition of I&C system design, plant functions, and hazards. Figure 5 illustrates the Beltracchi analysis framework in which function groupings are established and hazard classes are indicated. A high-level breakdown of a generic DI&C system is provided in terms of hardware, software, and human interfaces. Input, output,

and human-system interface functions are also treated. Within each functional grouping, critical characteristics (e.g., redundancy, diversity, independence, defense-in-depth) are identified to guide design assessment of the safety properties provided by the I&C system requirements. The purpose of the Beltracchi framework is to support analysis of I&C system requirements to assess safety characteristics (e.g., integrity) so it is not readily adaptable to the organization of function information within an inventory. However, the grouping of function according to a system breakdown has merit and the identification of critical characteristics within the functional–physical framework at the lower level of the abstraction hierarchy could be incorporated in a more suitable overall structure.

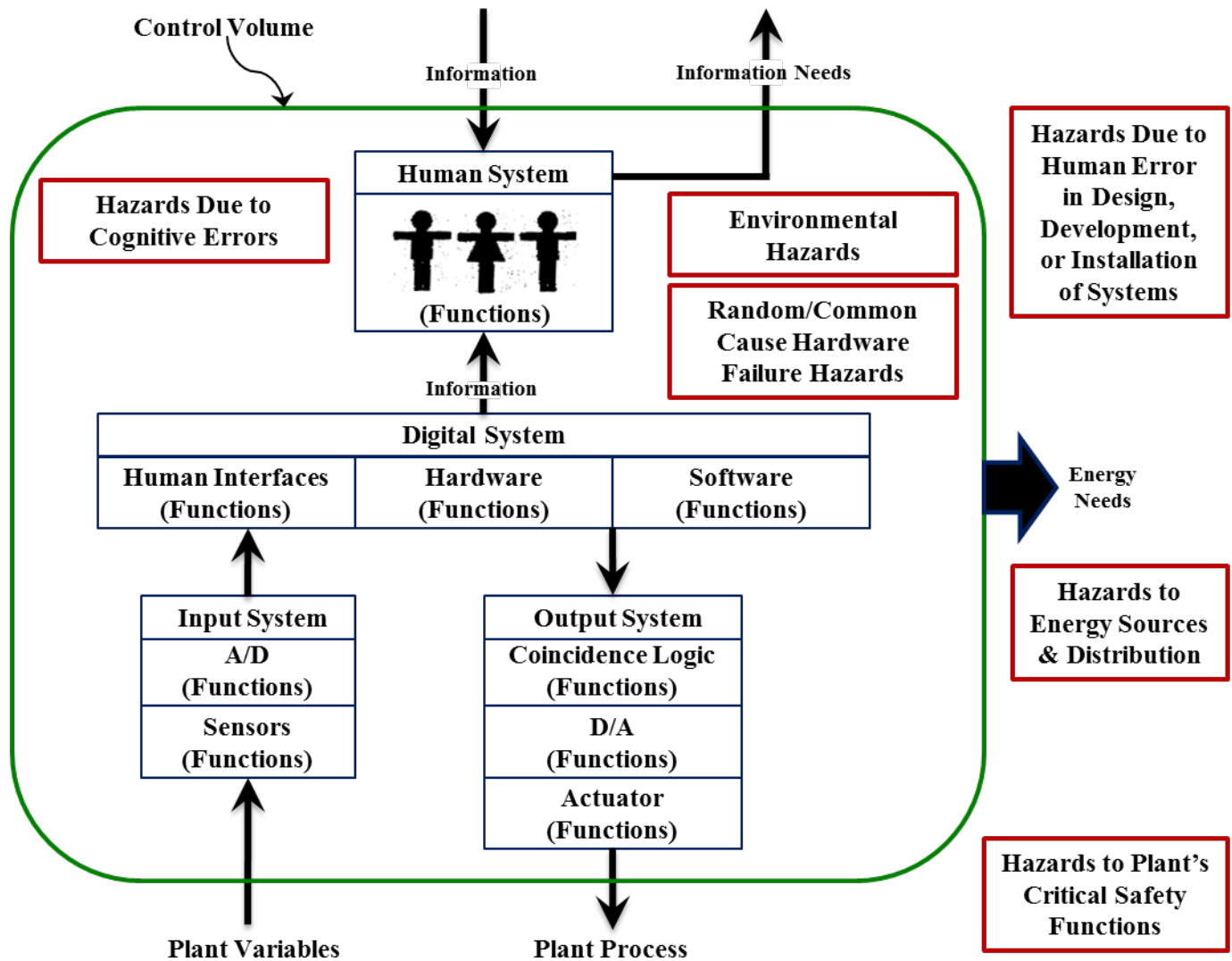


Fig. 5. Beltracchi analysis framework.

A more detailed, concrete representation of plant function, organized to reflect the physical configuration in the I&C architecture of an NPP, was developed under EPRI research intended to establish a DI&C inventory. In 1992, Babcock and Wilcox (B&W) Nuclear Service Company was engaged by EPRI to conduct a survey of the application of advanced technologies to systems within NPPs. This research effort involved development of a questionnaire to identify the use of advanced I&C and control room technology. The questionnaire was distributed to representatives of numerous domestic NPPs, but it is

unclear whether any plants participated in the survey. There is no publication available that documents survey findings from this activity and, based on inquiries with current EPRI personnel, any data that might have been acquired does not appear to have been preserved. Nevertheless, the questionnaire itself serves as an example of a function-based approach to organizing inventory information.

The B&W questionnaire solicited information about individual digital applications at the participating plant. In addition to the series of application-specific questions, the survey identified a functional breakdown of plant systems. The function-based representation of I&C systems involved the following categories:

- reactor protection and engineered safety,
- control and monitoring of principal plant systems,
- control and monitoring of plant support systems,
- emergency response,
- human-machine interface,
- voice and data communications,
- work management,
- plant historical data management, and
- access control/security.

For the EPRI-sponsored survey, information was solicited for DI&C system implementations in each function category. The questions were devised to capture data that included a general description of the application, key architectural features of the DI&C system, aspects of the software and hardware design, data processing and management approach, human-machine interfaces, and implementation/operational experience. Thus, the primary organization of information according to a functional representation incorporates not only design and configuration data items, but also information on the modernization approach used to implement the function using digital technology.

To support capture of implementation experience information, the survey included a structure to enable identification of survey information in terms of the lifecycle phases of a modernization project. The elements of the lifecycle framework indicated by the questionnaire are

- Design
 - requirements
 - industry standards
 - design bases
 - configuration/design control
 - design integration
 - vendor technical support
 - modification process
- Construction
 - scheduling
 - procurement
 - installation
 - testing
- Operation
 - training
 - startup

- normal operation
- emergency operations
- performance monitoring
- control modes/strategies
- alarm response
- Maintenance
 - preventative
 - corrective
 - surveillance/calibration
 - online testing/self-testing
 - spare parts
- Licensing/Regulatory
 - construction/operating license(s)
 - safety concern identification/resolution
 - audit

The lifecycle-based framework is suitable to allow information on modernization approaches and experience to be included within the function-based organization of survey findings, along with design and configuration data. The addition of information on modernization projects in parallel with the system-specific data could facilitate identification of best practices. However, it is noted that project modernization information constitutes another level of detail beyond the basic survey information that was readily identified in the initial inventory effort under this project.¹ Thus, a lifecycle representation of DI&C system information may be adaptable as a substructure within the organization of data in an expanded inventory or may be more suitable as the primary organizational structure for a parallel data collection specifically addressing modernization project experience.

The inventory initiated by the EPRI project was apparently never established so a fully realized database structure is not available. However, the organization of information according to plant function, as is implied by the questionnaire, can be considered in devising a classification framework under the current effort. This investigation of classification approaches based on functional representations also suggests other facets of information grouping that merit consideration. As seen in the various approaches investigated, a clear understanding of the relationship between abstracted data and the actual DI&C system is facilitated by maintaining close correlation between function and plant I&C architecture (i.e., coupled functional and physical representations) in the organization of information. Additionally, the association of critical characteristics with functional (or physical) groupings (e.g., classes), such as for the Beltracchi framework, can support analysis of the data for features that are important relative to safety or performance issues.

2.4 Critical Characteristics

Systems can be represented in terms of their properties, features, and qualities. A classification approach based on critical characteristics is common in many fields, such as systems engineering, biology, physics, sociology, etc. Weinberg¹⁶ described systems according to three categories based on characteristics of randomness and complexity. The categories are described as *organized simplicity*, *unorganized complexity*, and *organized complexity*. Systems with low degrees of complexity and randomness fall within the organized simplicity category. These systems are characterized by simplicity and organization such that they can be readily decomposed by analytic reduction into noninteracting subsystems. Systems with a high degree of randomness are grouped within the unorganized complexity category. These systems typically do not display an easily identifiable underlying structure and are not readily subject to

decomposition. Instead, these systems may be represented as aggregates of interchangeable elements whose behavior can be treated in terms of average properties through statistical analysis. The systems within the remaining category, organized complexity, are too organized to be treated solely in terms of statistical properties and too complex to be reduced and thoroughly analyzed. Complex software is an example that fits within the organized complexity category, in which both statistical and reduction analyses are each insufficient to solely address the full range of design and assessment issues posed by software-based systems.

Treatment of systems within the organized complexity category falls to methods developed under systems theory. In this approach, complex systems are represented hierarchically with control processes establishing the primary interfaces between levels.¹⁵ Effectively, control laws impose constraints from higher levels of the hierarchy on system/component behavior at lower levels. In the Systems-Theoretic Accident Model and Processes (STAMP) framework for analyzing accidents, Leveson¹⁷ established an approach to classifying accident factors in terms of control loop and process models. These models enable constraints and levels of control to be represented in terms of a typical control loop structure. In addition to a controller, actuators and sensors, and the controlled process, the human supervisor is also represented. Displays and controls provide the interfaces between the controller and human supervisor while measured and controlled variables provide the interfaces between the controller and controlled process, through the sensors and actuators, respectively. Capturing the causal factors that lead to accidents in terms of flaws incorporated into the components of the control loop at various lifecycle phases (e.g., design, development, manufacturing, operations), Leveson classified control flaws leading to hazard in three categories: (1) inadequate enforcement of constraints (i.e., insufficient control), (2) inadequate execution of control action, and (3) inadequate or missing feedback. Each category is further decomposed into more specific sources of flaws. The STAMP framework is intended to facilitate accident analysis by including representation of the control structure itself in the assessment of what flaws are present and why an event occurred.

Failure analysis frequently involves classification of systems and faults in terms of critical characteristics. Laprie¹⁸ established a tree structure to define dependability characteristics for a system. The dependability branches are attributes, means, and threats. Attributes of dependability include properties such as availability, reliability, safety, confidentiality, integrity, and maintainability. Means of achieving dependability include fault prevention, fault tolerance, fault removal, and fault forecasting. Threats to dependability are characterized as faults, errors and failures. Laprie further classified faults and failures according to tree structures. Faults are classified according to five categories, which are phenomenological cause (e.g., physical and human-made faults), nature (e.g., accidental, intentional nonmalicious, and intentional malicious faults), phase of creation or occurrence (e.g., developmental and operational faults), system boundaries (e.g., internal and external faults), and persistence (e.g., permanent and temporary faults). Failures are classified according to three categories, which are domain (e.g., value and timing failures), user perception (e.g., consistent and inconsistent or “Byzantine” failures), and consequences on environment (e.g., benign through catastrophic failures). Lala and Harper¹⁹ adapted the fault classification approach by Laprie to address common-mode failure (CMF). Lala and Harper grouped the phenomenological cause, phase of creation, and system boundaries categories as subelements of a higher-level classification by origin. Thus, common-mode faults are classified according to nature, origin, and persistence. Treatment of CMF follows by relating the fault classification to a classification of CMF sources (i.e., common-mode faults that lead to CMF). In their taxonomy for CMF, Lala and Harper exclude consideration of intentional faults based on the prevailing condition that security had not often been treated as a requirement for ultra-reliable real-time applications. Five classes of CMF were defined in terms of transient externally induced faults, permanent externally induced faults, intermittent design-related (i.e., lifecycle) faults, permanent design-related faults, and interaction (i.e., human-system interaction) faults. Lala and Harper note that methods to address common-mode faults typically rely on one of the primary means of achieving a dependable system. Specifically, treatment of CMF typically involves fault-avoidance techniques during early lifecycle phases (e.g., specification, design and

implementation), fault-removal techniques during later lifecycle phases (e.g., test and validation), and fault-tolerance techniques during the operational lifecycle phase.

Hawthorne and Perry²⁰ treat the methods of addressing common-cause failure (CCF) in dependable systems by classifying types of diversity and establishing an architectural framework to capture top-to-bottom design diversity. The architectural framework of Hawthorne and Perry incorporates the whole system by representing hardware, software, and infrastructure. A physical representation is adopted for a high-level model of hardware elements (processor, memory, etc.), software elements (applications, layered software components such as utilities and system services, operating system, etc.), and architectural infrastructure (networks, power, etc.). Diversity-enhancing properties of the system design are classified as modal diversity, geographical diversity, and ecological diversity. Modal diversity provides for diverse modes of accomplishing system functions (e.g., functional diversity). Geographical diversity involves distributing hardware/software components to avoid localized failures due to environment and other external influence factors. Ecological diversity can be achieved by employing dissimilar hardware, software, networks, and other infrastructure components to protect against platform or technology specific vulnerabilities. Other diversity properties, such as temporal, control, and combinational diversity, were identified as potential classes. Specifically, combinational diversity involves using unique, but not necessarily mutually exclusive, sets of diversities across multiple parallel systems (e.g., diverse redundant channels). Essentially, the combination of diversity-enhancing properties would vary from channel to channel to achieve this class of system-level diversity.

In an assessment of OpE insights into CCF for DI&C systems, EPRI TR-1016731 [Ref. 21] identifies groupings of cause for common defects. These groupings include incorrect parameter value, single point vulnerability, hardware failure, manufacturing defect, inadequate requirements definition, inadequate hardware design, inadequate software design, inadequate software verification and validation, inadequate testing, inadequate operating procedures, inadequate maintenance procedures, inadequate vendor information, inadequate training, operator error, maintenance error, human performance, ineffective configuration management, ineffective change management, and ineffective vendor oversight. In addition, based on an analysis of failure for both Class 1E and non-Class 1E systems, the EPRI investigation identified key design attributes that can affect CCF mitigation. These design characteristics include redundancy, shared resources, signal diversity, functional diversity, use of formal software quality assurance methods, functional complexity, and system interactions.

The NRC Common-Cause Failure Database and Analysis System (CCF DAS) at Idaho National Laboratory established a classification structure to capture the main elements of CCF events.²² Nuclear power plant I&C systems are classified into four categories (i.e., system, components, subcomponents, and piece parts) based on a whole-part decomposition. Events are classified in terms of component fault state (i.e., available or unavailable), cause, and coupling factor. The coding system for component fault state decomposes into “no failure” and “potentially unavailable” (expanding into “potentially failed” and “potentially functionally unavailable”) for the “available class” and “failed” and “functionally unavailable” for the “unavailable” class. Failure causes are grouped as proximate cause or root cause. Associated conditioning and triggering events can also be identified. Major categories established within the cause class include state of other components, design/manufacturing/construction inadequacy, abnormal environmental stress, human actions/plant staff error, internal, procedure inadequacy, and unknown. Coupling factors are classified as hardware based, operation based, or environment based. Defense mechanisms to address CCF are identified according to their prominent characteristic, such as functional barrier, physical barrier, monitoring and awareness, maintenance staffing and scheduling, component identification, diversity, unknown, and no practical defense. Assignment to these classes is based on analysis of events extracted from failure and event databases.

NRC RES staff²³ documented an initial investigation of classification approaches that could serve to support evaluations of OpE and investigations of strategies to address CCF vulnerabilities. As part of this effort, an approach was proposed for classifying DI&C systems based on critical characteristics that are

relevant to interpreting OpE. Arndt²⁴ further described this classification approach and discussed how it could be employed to determine the level of detail in reliability modeling that would be necessary to support performance-based regulatory treatment of DI&C systems. As described below, the three-attribute taxonomy for classifying DI&C systems in terms of critical characteristics incorporates concepts from other classification approaches. In particular, the NRC approach, documented by Arndt, builds on concepts reported by John Rushby, Charles Perrow, and Tunc Aldemir.

Rushby²⁵ documented an approach to classifying critical properties of systems in a systematic taxonomy. In particular, Rushby analyzed representations of critical system properties from the standpoint of dependable systems, safe systems, secure systems, and real-time systems. Rushby noted that the taxonomy for critical systems must address the condition that “modern systems are often required to satisfy two or more critical system properties simultaneously” and, thus, design aspects such as security, fault tolerance, real-time performance, and safety must be considered.

Rushby adopted two attributes identified by Perrow²⁶ as the basis for an organization of critical system properties. These attributes are “interaction” and “coupling.” The interaction attribute characterizes the degree to which the behavior of a component in a system can impact the behavior of other components. Interaction is expressed in terms of complexity, ranging from linear to complex behavior. The coupling attribute characterizes the extent to which system(s) behavior is rigid or flexible (i.e., tightly coupled or loosely coupled, respectively) in relation to factors such as input order, timing, execution sequence, etc. Although the assessment of system properties according to the two principal attributes is subjective in nature, the Rushby approach does enable classification of systems in terms of the degree of interaction and coupling exhibited through their critical design characteristics.

In NUREG/CR-6901, Aldemir²⁷ developed a taxonomy for failure modes of DI&C systems that more fully resolves the interaction attribute while clarifying the coupling attribute. Basically, the determination of what constitutes loosely coupled and tightly coupled is more completely defined by establishing subattributes for interaction. Aldemir defines Type I and Type II interactions in which the former addresses interactions among DI&C systems and the plant processes that are controlled by the systems while the latter addresses interactions (e.g., communication, multitasking, multiplexing) within digital systems. Type I interactions can produce statistically interdependent failure modes due to the coupling of system performance through plant processes. Type II interactions can result in failure modes that originate from the coupling among systems and components (e.g., hardware, software, firmware).

The NRC classification approach extends the concepts of Rushby, Perrow, and Aldemir by establishing a DI&C system representation in terms of system complexity, system interaction/interconductivity, and system importance. System complexity is based on Type II interactions and other indicators of system size and complexity (e.g., function point or cyclomatic complexity metric). The intention is to capture intrinsic interactions between digital system elements such as hardware, software, and firmware and the overall complexity of a DI&C system. System interaction is based on Type I interactions and system coupling. This attribute deals with extrinsic interactions for a system with the plant and with other systems. It addresses functional and physical interconnections and dependencies among systems and differentiates between tightly coupled and loosely coupled systems. System importance is based on importance measures that include traditional safety and risk metrics as well as indicators of significance toward maintaining key design and operational concepts (e.g., defense in depth). The application of the NRC classification approach involves characterization of a DI&C system in terms of each of the three attributes, which range from simple to complex, loosely coupled to tightly coupled, and low importance to high importance. This approach was demonstrated in a conceptual example reported in Ref. 24 in which a generic reactor protection system (RPS) and generic digital feedwater control system (DFWCS) are classified. The RPS is expected to exhibit relatively high-risk importance but low complexity. The DFWCS is expected to show relatively low importance but much higher complexity and interaction. The approach to classification is illustrated in Fig. 6, which is drawn from Ref. 24.

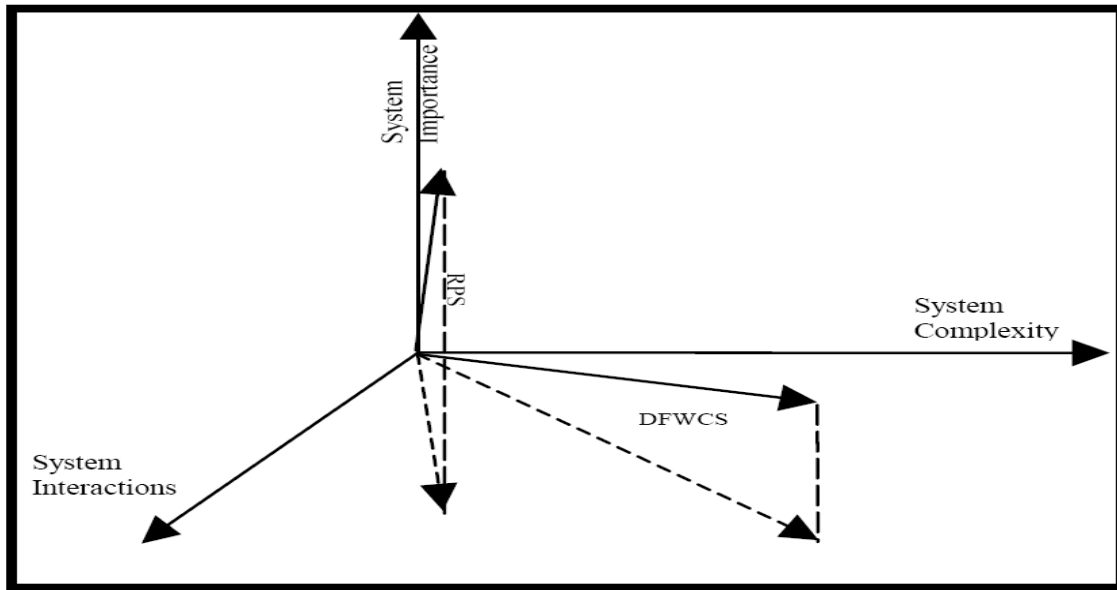


Fig. 6. Conceptual classification of DI&C systems.

The investigation of classification structures that involve categorization based on critical characteristics suggests an approach that can provide the potential benefit of grouping DI&C systems in terms of properties or qualities that are of primary interest in OpE analyses. However, it is observed that these approaches generally suffer from two weaknesses. First, many of the characteristics identified in the classification approaches that were studied are highly subjective in nature (e.g., complexity, diversity) and do not have well-defined classes or comprehensive measures. Consequently, a subjective assessment of DI&C systems is necessary that may often be limited to coarse categorization based on yes/no, high/low, or other similarly rudimentary value judgments. Clearly, an approach focused on tangible or objective criteria for categorization is best suited to provide a predictable basis classifying DI&C systems.

A second perceived weakness of the critical characteristics approach to classification is the abstract nature of the categorization. In many cases, the relationship between class structure and the physical system is highly obscured by the degree of abstraction. While sorting and portrayal according to observed or inferred characteristics is reasonable for organizing system information, the inverse process of reconstituting concrete details of a DI&C system from a depiction based on intangible features can be a severe challenge. Thus, to be directly useful in establishing a classification framework suitable for treatment of system information within a DI&C inventory, a direct tie between the physical realization of a system and representative classes based on less tangible critical characteristics is warranted.

2.5 Conclusions

The investigation of classification structures identified several classification frameworks ranging from high-level abstractions to basic descriptive representations. As noted, the primary classification approaches used in the international nuclear industry involve categorization of systems and functions based on safety importance. The objective of the classification structure recommendations arising from this research is not to revise or supplant the current safety classification approach, but instead the research is intended to provide a classification structure to support the development of an inventory of DI&C systems. Thus, any classification approach developed for treating DI&C system information must be compatible with and complementary to the existing safety classes. It was noted that incorporating a safety

class (or category) identifier as a data element associated with each implemented system captured in a DI&C inventory can enable safety significance to be represented.

During the review of the classification frameworks, it was observed that, as the degree of abstraction increased, the tie between constituent classes or categories and the physical aspects of a system becomes less direct. Thus, the classification structures tended to become less intuitive as the level of abstraction increased. Consequently, it was concluded that a more tangible, less abstract structure would be most effective and usable.

It was also observed that a physical representation provides a basis for organizing information about DI&C systems preserves a relationship with the installed I&C systems. However, features and capabilities, such as software and human interfaces, strongly depend on recognition of function and critical characteristics that cannot be fully represented solely on the basis of a physical model. As seen in the various approaches investigated, a clear understanding of the relationship between abstracted data and the actual DI&C system is facilitated by maintaining close correlation between function and plant I&C architecture in the organization of information. Additionally, the association of critical characteristics with functional (or physical) groupings can support analysis of the data for features that are important relative to safety or performance issues.

Based on the findings of the investigation of classification approaches, a classification structure that enables physical, functional, and critical characteristic information to be captured and interrelated seems most suitable to provide the structure for a DI&C inventory to support OpE and other system analyses. Accordingly, a classification framework should incorporate a coupling between physical and functional representations within a hierarchical abstraction as a basic structural element. The following section describes the recommended classification structure developed through this research.

Page intentionally blank

3. CLASSIFICATION STRUCTURE

The approach to classification that is presented in this section focuses on a structure that is relevant for the type of information that can realistically be gathered from available resources about the range of DI&C systems currently installed in domestic NPPs. The findings from an investigation of DI&C systems at NPPs in the United States are documented in a companion letter report.¹ The information obtained through that investigation primarily consists of identification of the I&C systems at specific plants that are based on digital technology, coupled with identification of the digital platform used. This information composes the basic inventory data compiled by plant from the initial study.

By considering the data that would likely be available in the near term, the objective of this research effort to develop a classification structure focused on how best to accommodate organization of DI&C system data consisting of the following classes of information:

- system,
- function, and
- platform.

These very high-level information groupings form a three-leg representation of the expected primary information for a DI&C inventory and comprise the basic structure for the classification approach devised in this research:

1. the identification of system constitutes an architectural (or physical) view of the DI&C inventory;
2. the identification of function represents a functional view of the DI&C inventory and can account for the safety classification assigned to each DI&C system; and
3. the identification of platform (i.e., supplier and product identifier) represents a technological view of the DI&C inventory.

Each of these views of DI&C system information constitute sets of data that share common attributes; therefore, they can be treated as classes of information that can be interconnected based on relationships among the attributes of the different information classes.

Cataloging DI&C systems in terms of these three classes retains a connection to the actual organization of the systems in the plant, the purpose and significance of the systems, and the source and nature of the system deployment (i.e., implementation of a platform). Information about the system and platform corresponds to the physical architecture of the DI&C systems in a plant and the use of digital technology to implement these systems. The information about function can be derived from the safety classification and functional requirements of each system.

The detailed component-by-component, feature-by-feature data that corresponds to each of the primary classes can be extensive. Therefore, as a practical matter, organization of information classes to support the collection of data has to be treated with some level of abstraction. Systems and functions can be abstracted (determined) from detailed, plant-specific naming, configuration, and functional allocation data to more general system and functional groupings, as is discussed below. Platforms can be grouped on a practical level by vendor or can be treated in terms of common technologies, implementation approaches, performance capabilities, or other identifiable characteristics.

Although abstraction is employed to reduce complexity in classifying DI&C systems, the classification structure must also be sufficiently flexible to allow the granularity in the groupings to be more finely resolved to support more detailed investigations. In each of the primary classes, attributes that represent key components, characteristics, or features can be established and used to form the basis for an expanded representation of the data. Identification of general attributes along each leg of the classification structure

can be further resolved into more detailed attributes that provide greater discrimination among data items. This suggests a hierarchical approach to organizing data collections for the DI&C inventory that allows high-level abstraction at the upper levels of the hierarchy and detailed representations at the lower levels of the hierarchy.

The following subsections address each of the three primary information classes for the classification structure, with a focus on the organizing the information into attributes that provide more details on a given DI&C system.

3.1 System Class

Identification of systems as a principal aspect of a DI&C inventory involves determination of which plant I&C systems use digital technology. Thus, the system class for the classification structure consists of a catalog of specific applications of DI&C systems for each plant. The listing of those I&C systems that employ digital technology constitutes the fundamental basis of the DI&C inventory. The basic information within this class, grouped according to plant by unit, can include:

- system designation (e.g., generic type or plant-specific name);
- service dates (i.e., installation/commissioning);
- system/platform supplier; and
- digital platform identification (i.e., product name, model number, version number).

The most straightforward approach to organizing system information is to adopt a data abstraction based on a physical representation that retains a direct relationship with the plant I&C architecture. As discussed in Sect. 2.2, a whole-part abstraction is an abstraction approach based on a hierarchical decomposition of physical systems to provide a manageable representation of a comprehensive system architecture. At the highest level, the plant I&C architecture can be decomposed into systems. The hierarchical representation of the system information can extend to lower level decomposition of each system into its constituent parts (e.g., subsystems, modules, components, piece parts).

For the topmost level corresponding to the plant I&C architecture, the representation hierarchy for the whole-part abstraction within the system class can adopt a generalized system taxonomy. As previously noted in Sect. 2.2, the system codes for the SCSS provide 18 types of systems for categorizing LERs addressing I&C systems. Volume 1 of EPRI TR-103699 (Ref. 11) identifies four categories of systems: nuclear steam supply system (NSSS) safety Class 1E systems (protection), NSSS nonsafety systems (control), balance of plant (BOP) safety Class 1E systems, and BOP nonsafety systems. These categories are further resolved into generic systems within each grouping based on a general pressurized-water reactor (PWR) design and a general boiling-water reactor (BWR) design. In Appendix A, Table A.1 gives the catalog of systems for a BWR while Table A.2 gives the catalog of systems for a PWR.

At lower levels of the hierarchy based on the whole-part abstraction, an item (e.g., system, subsystem, module, component) can be decomposed (further subdivided) in terms of a block structure that captures key architectural features of DI&C systems. The structure for representing an item at a particular level of the hierarchy involves a primary computational element, input element, output element, human interface element, and interconnected external elements (see Fig. 7). This approach to representing a decomposed system is intended to capture information about the physical structure and interconnections of the DI&C system in terms of the plant I&C architecture or system configuration. For a DI&C system, the primary computational element would be the digital platform upon which the plant function is implemented. Clearly, input and output elements would include sensors and actuators. The human interface element includes displays, input devices, and any other system-level human-machine interfaces. External elements include interconnected systems and components (other than inputs and outputs) that are not considered part of the system. The first three blocks provide an end-to-end representation of an I&C system (e.g., a

safety channel or single-loop controller) while the human interaction block represents the means for human-system interaction. The external element block supports a representation of architectural interconnections between and among systems.

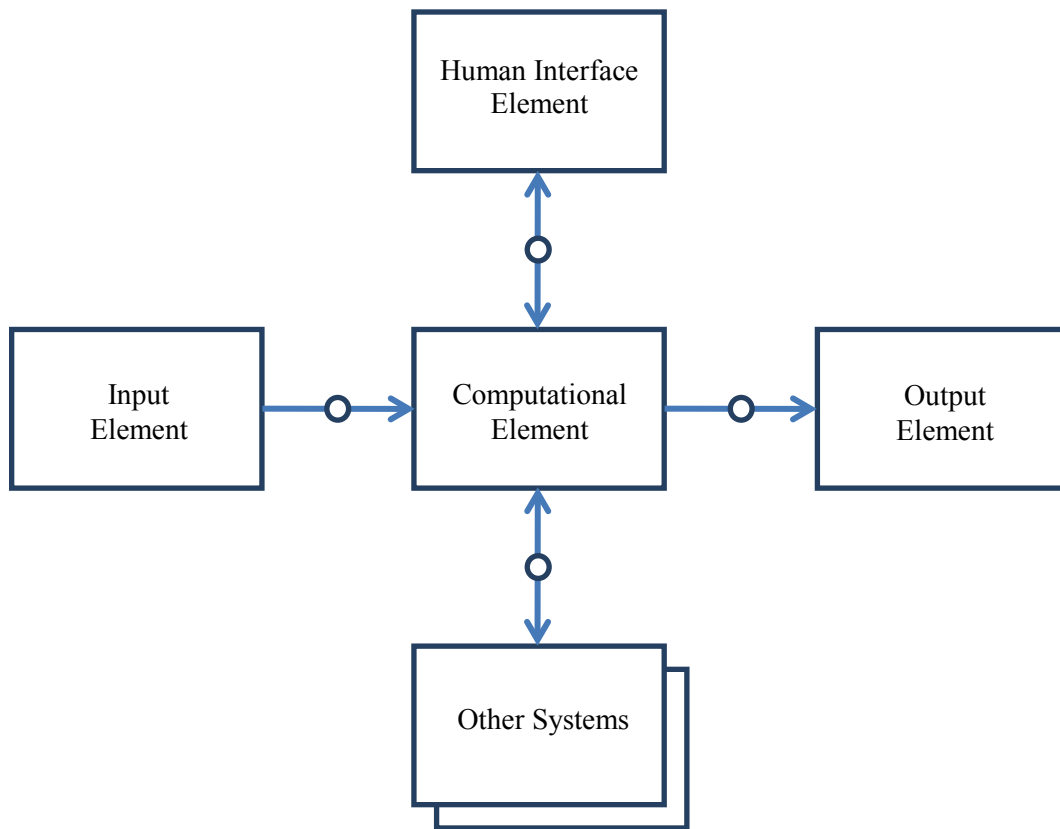


Fig. 7. Structural representation of system architecture.

In terms of a physical model of the system, decomposing the computational element for a DI&C system can expand the physical representation of the system to include subsystems, such as independent parallel divisions or channels of a safety system or individual control loops within a distributed control system. Alternately, the decomposition of the computational element can represent the internal structure of a platform, with the subelements consisting of racks within a cabinet or modules within a chassis. Further decomposition can address components at the board level. At those lower levels, the data organization of the system class corresponds directly with the categories of hardware component attributes established within the information structure of the platform class.

Further decomposition of a DI&C system requires increasingly detailed knowledge about the design, implementation, and architecture of that system and the platform on which it is based. A practical approach is to begin with a high-level system catalog for each plant and expand the information collection for the system class by capturing plant-specific information on the overall I&C architecture with its system interconnections, as it becomes available. Capture of more detailed knowledge regarding internal system architectures (e.g., processor, bus structure, execution environment, software usage) can be supplemented by implementation-specific information on platforms obtained through topical report submissions or responses to vendor-specific surveys. As discussed below, this data can be organized according to platform in terms of attributes (i.e., key characteristics or features) within the information structure of the platform class.

It should be noted that the block structure for representing system information is not restricted to identification of hardware components. Each element can include data attributes such as function, plant location (e.g., containment, BOP, equipment room, control room), service environment, and so forth. Additionally, expansion of any computational element can be resolved into software or functional structures as well as hardware structures. Figure 8 illustrates the expansion of the computational element into more detailed presentations of information about an I&C system at a particular level of the decomposition hierarchy. In the figure, the upper expansion illustrates how more information could be displayed about the software structure for a digital implementation of an I&C system. The lower expansion indicates how more detail about the hardware components and configuration could be displayed. Similar expansions are possible for the other elements of this five-block representation. This flexibility in representation supports organization and presentation of more detailed information so that it can be related upward through the hierarchy to particular I&C systems (i.e., to support detailed searches of a given I&C system).

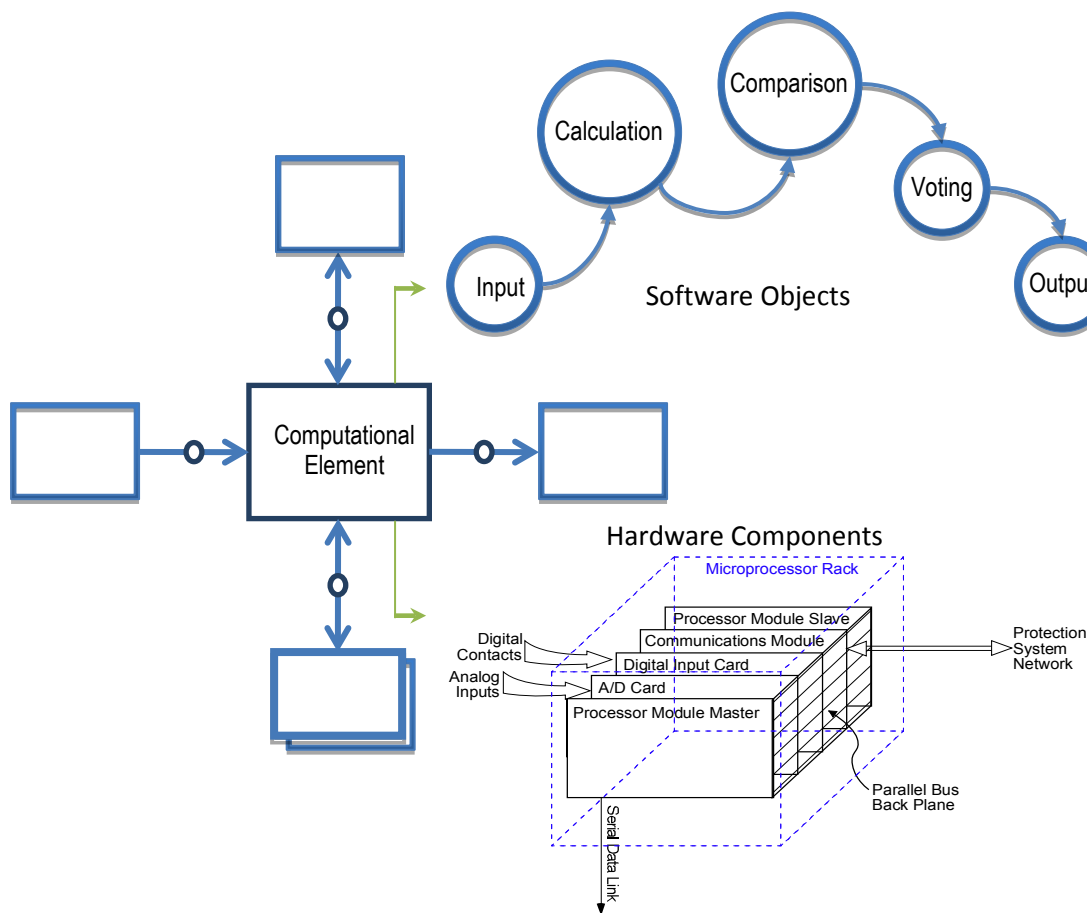


Fig. 8. Expansion of block representation to illustrate presentation of greater detail.

3.2 Function Class

Identification of functions as a principal aspect of a DI&C inventory involves determination of which functions are implemented digitally. The function class for the classification structure corresponds to the plant functions embodied in DI&C systems and the digital functionality used to implement those plant functions. Capturing plant function information establishes a context for relating DI&C systems in terms of significance. Essentially, the purpose of an I&C system is defined by the plant function(s) it performs

or supports and these functions determine its significance in terms of safety, investment protection, or economic performance.

To support generation of a DI&C inventory, information on plant functions can be captured based on engineering knowledge of typical plant I&C system architectures, documentation of safety analysis and event reports, and the identification of functions by safety importance. The existing safety classification of plant functions indicates the significance of their role in ensuring the integrity of the barriers to the release of radioactive material to the environment and can be treated as a key attribute of each plant function identified within this information class.

The allocation of plant functions to digital technology can be related to an architectural representation at the plant level, system level, and subsystem, module, and component level(s). Establishing a relationship between the function and the I&C system enables a direct connection between data items in the function class and data items in the system class. A further breakdown from system-related functions to specific functionality provided by hardware/software elements of a digital platform depends on the specific application, implementation architecture, and platform capabilities. The digital functionality relates directly to the function attribute established within the information structure of the platform class.

At the plant level, functions relate to system objectives (i.e., specific purpose) and the means to accomplish those objectives (i.e., characteristic action). As noted, the significance of a plant function is characterized in terms of its safety classification. However, the characterization of the means by which plant functions are realized is highly coupled to the distribution of those functions within the I&C architecture of a plant. A common way to subdivide the I&C architecture of a plant by functional groups is the following:⁷

- sensors to interface with the physical processes within a plant and to continuously measure plant variables;
- operational control, regulation, and monitoring systems to process measurement data for managing plant operation and optimizing plant performance;
- protection systems to keep the plant in a safe operating envelope in response to any postulated initiating event (e.g., design basis accident);
- communication systems to provide data and information transfer through wires, fiber optic cables, digital data buses, or wireless networks;
- human-machine interfaces (HMIs) to provide information to and interaction with plant operating personnel; and
- actuators (e.g., valves and motors) to respond to commands by the control and safety systems to adjust the plant's physical processes.

This approach to attributing plant functions according to the plant I&C architecture enables a physical-functional coupling to be established. At the highest level of abstraction, plant functions can be characterized according to purpose as protection, control, or monitoring. Supporting functions include measurement, actuation, communication, computation, and human interaction (e.g., display and interface). Protection functions can be further resolved into reactor shutdown (reactivity control), heat removal (reactor core cooling and inventory control), primary pressure boundary integrity protection, radioactivity control, and containment integrity and isolation. A breakdown of control and monitoring functions includes power (reactivity) control, pressure control, coolant inventory control, coolant chemistry control, core heat removal, heat sink control, flux monitoring, radiation monitoring, leak detection, information display, and alarms.

Figure 9 illustrates a functional–physical representation that can be applied to the protection, control, or monitoring functions allocated in I&C systems. This approach adopts a structure that is reflective of an instrument string (see Fig. 1) and is consistent with the block representation described in the previous

section (see Fig. 7). The computation function shown in the figure represents the principal implementation of a protection, control, or monitoring function, which would be realized as a system either by a string of analog modules or an application based on a configured (e.g., programmed) digital platform. For a digital protection system, the protection function (i.e., trip determination) would be implemented using the computational functionality of a digital platform. The measurement and actuation functions would generally be associated with sensors and actuation devices while the communication function could be digital or analog (e.g., serial or networked interconnections vs. hardwired signal transmission). The human interaction function could involve displays and/or interface devices as peripherals or through a separate human-machine interface system (e.g., operator workstation).

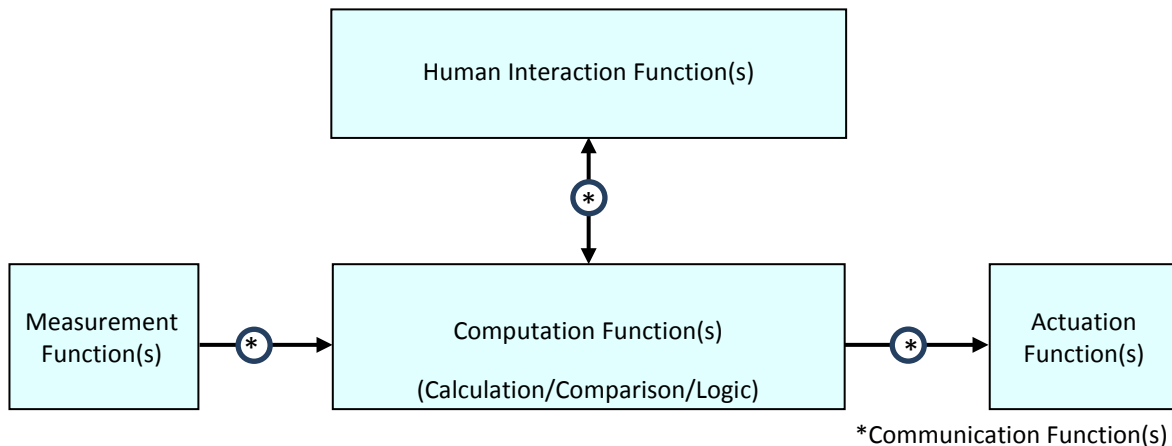


Fig. 9. High-level functional–physical representation of a plant function.

A more extensive catalog of plant functions can be generated based on generic descriptions of plant functions for various reactor types. Volume 2 of EPRI TR-103699 (Ref. 12) provides a technical description of safety and nonsafety functions for the NSSS and BOP of a general PWR design. A list of those PWR functions is included in Appendix B. More detailed catalogs of functions such as provided in Appendix B can serve as a suitable expansion of the higher-level groupings identified above and allow for more detailed sorting of plant function.

The granularity of the plant function representation in the classification structure can be treated hierarchically according to a layered whole-part abstraction approach, with high-level groupings expanding into more detailed breakdowns of function. This approach can be visualized as a root system, with each higher-level category (e.g., protection) branching into lower-level categories (e.g., shutdown, heat removal, pressure boundary integrity, radioactivity control, containment integrity and isolation). As the progression through this leg (root stem) of the classification structure proceeds to lower levels of the hierarchy, the representation of function becomes more detailed until the attributes becomes less general and more specific to a particular function or its underlying functionality. As the DI&C inventory evolves, new functions can be added and a finer breakdown of function to its constituent functionality can be introduced.

The DI&C system functions can be further decomposed into constituent functionality elements. These include data acquisition, actuator activation, communication, arbitration, control, limitation, commanding, validation, checking, monitoring, prediction, fault management, and configuration management. It is noted that not all of these functionalities are present within every DI&C system nor are they necessarily implemented in the I&C architecture of any particular NPP.

Identification of functionality embedded within DI&C systems requires an understanding of the detailed design, architecture, and allocation of function. High-level groupings in terms of primary functionalities can be achieved based on an understanding of the nature of the function implemented in the DI&C system but finer granularity in classifying functionality necessitates detailed information about system implementation (in particular, the platform functionality) to be feasible. Achieving information capture and organization to this extent can be a long-term goal as a basic inventory of DI&C systems is developed and evolved. As noted, a hierarchical classification structure allows expansion to include greater levels of detail.

3.3 Platform Class

Identification of digital platforms as a principal aspect of a DI&C inventory involves determination of which products are implemented and what digital technology is employed. The inventory data within the system class should include the platform/product identification as a data attribute of each captured instance of a DI&C system. This primary data attribute within the information structure of the system class is associated with platform-related attribute categories within this class of information. These attribute categories established for the platform class provide an information structure to capture the critical characteristics and key capabilities for each platform that is investigated.

The platform information should capture the technology used. Examples of digital technology include software-based systems such as computers (general purpose microprocessors), programmable logic controllers (PLCs), and microcontrollers or logic-based systems such as complex programmable logic devices (CPLDs) and field programmable gate arrays (FPGAs). The platform information should also indicate the extent of the implementation, which could include full system (monolithic or distributed), module or component (e.g., local single-loop controller, display interface, communications node, priority module) of a system or embedded component (i.e., microprocessor for smart sensor, smart actuator, uninterruptable power supply, etc.).

3.3.1 Investigation of available platform information

The organization of information for the platform class within the DI&C system classification structure consists of data attributes associated with each platform. The set of recommended attributes is drawn from the investigation of critical characteristics identified in safety evaluation reports (SERs) and those descriptive properties or features captured for digital platforms in other industry surveys and reports. These attributes are not intended to represent a comprehensive set of characteristics but serve as a starting point that can be expanded through the introduction of additional attributes as more information becomes available. In addition, these attributes represent high-level characteristics that can be resolved into greater detail through decomposition into subattributes and/or finer resolution of the attribute data (i.e., a more detailed representation of a feature or property, such as expanding the interconnections attribute grouping by identifying various forms of network communications used for external interfaces).

As discussed in Sect. 2.2, EPRI conducted a survey of digital I&C platform vendors in the late 1990s. Nine vendors responded to the survey with varying degrees of technical detail about their product lines. The specific platforms described in the report¹³ are as follows:

- ALSPA 8000-P320 by ABB Alstom Power (formerly CEGELEC),
- *SPINLINE 3* by Schneider Electric,
- Neutron Flux Monitoring System by Gamma-Metrics,
- Control STAR by Framatome Technologies (now AREVA ANP),
- Symphony (*Contronics-S* and *INF1 90*) by ABB Automation,
- Advant Controller AC 160 by ABB Combustion Engineering (now Westinghouse),

- SPEC 200 Micro by Foxboro, and
- TOSMAP GS/DS by Toshiba.

The general categories of information captured from the survey included architecture (i.e., platform configuration), components (i.e., hardware and software), communications capabilities (e.g., networks, buses, datalinks), tools (e.g., development, engineering, simulation), standards compliance, and critical characteristics (performance, capacity, and dependability). The findings captured in this report are very high-level descriptions that can form rudimentary data sets for each platform. The categories of information described in the report identify attributes (i.e., features, characteristics, or properties) that can be incorporated into the platform class.

In order to further develop the data structure of the platform class, the information content contained in safety evaluations of topical reports on digital platforms was assessed. In particular, the SERs on the Teleperm XS,²⁸ Common Q,²⁹ and TRICON³⁰ platforms were reviewed. The purpose of this assessment was to identify key features and characteristics of digital platforms that were reported and given emphasis in the evaluations of the suitability of each platform for safety applications. On the basis of these identified characteristics, an initial set of information attributes for the platform class can be established. In addition, the platform specific information for each attribute constitutes a data resource within the platform class. This information can be collated as a database of key characteristics for each platform, which can then be interconnected by association of attributes among the platform-specific databases to support relational searches.

3.3.2 Attribute categories for the platform class

The attributes identified for the platform class within the classification structure for DI&C systems are derived from the investigation of platform information available from the sources described above. These attributes can be organized into several categories (see Appendix C). These categories are helpful in organizing the attributes and determining the coverage of identifiable features and critical characteristics provided by the attributes.

The discussion below describes the specific attribute categories developed through this research and provides examples of data items that can be compiled within this information structure. These attributes represent a organization of information that can be collected about digital platforms.

3.3.2.1 Architecture

Architecture attributes capture the physical and logical configuration of the platform and identify important design concepts used to implement systems. These design concepts include redundancy, independence (e.g., buffered communications through a separate communications module or processor), diversity, and fault management. For example, triple redundancy is a design concept that serves to isolate and mask random failures while enabling fault management through validation (e.g., signals, commands). The platform architecture attributes can be associated with the decomposed system attributes within the system class data set (i.e., inventory) to relate the plant architecture and system interconnections with the internal platform configuration. Again, specific implementation details can be captured in this manner if the information is available.

Physical arrangement: This attribute grouping addresses the internal architecture of the platform (e.g., racks, chassis card slots, modules, backplane) and identifies internal interfaces (e.g., communications, power, etc.).

Configuration management: This attribute grouping addresses information on identification of components and versions, access control, security, etc.

Fault management strategies: This attribute grouping can be decomposed to identify any design/implementation approaches employed for fault containment/isolation, such as independence, redundancy, defense-in-depth, diversity, etc., as well as specific methods used, such as signal validation, self-diagnostics, etc.

Watchdog timer protection: This attribute can identify the provision for watchdog timer protection and indicate the means of implementation (e.g., hardware, software).

Maintainability: This attribute grouping includes identification of provisions for testing, fault identification, and repair.

3.3.2.2 Hardware components

Viewing the platform as a collection of components, hardware component attributes identify the significant characteristics of the platform hardware. There are many subcategories of hardware that can be included so the range of attributes will depend on the degree of decomposition for which information capture can be achieved.

Types of modules/components: This attribute grouping captures the nature of each module (e.g., I/O, control, communication, display, etc.) and can be decomposed to components with key capabilities.

Technology basis: This attribute captures the technological basis for the platform in terms of the primary computational element. Examples include general-purpose central processing units (CPUs), microcontrollers, FPGAs, CPLDs, application integrated circuits (ASICs), and discrete component logic. This attribute also implies the degree of complexity at the microarchitecture level for the platform's main processing unit.

Digital processor identification: This attribute identifies the specific processor used in the platform by name (i.e., manufacturer and chipset family designation).

On-board memory: This attribute grouping captures the software and data storage capabilities provided by the platform. For each memory type, the technology (e.g., PROM, Flash, SRAM, DRAM) and capabilities (e.g., read-only, writable, dual-port access) can be indicated as well as the nature of the memory usage.

Nuclear-grade or commercial-off-the-shelf (COTS) components: This attribute indicates the pedigree of the identified components.

Environmental rating: This attribute indicates the expected ranges of service environments from controlled (mild) to severe (design basis accident conditions).

3.3.2.3 Software components

Viewing the platform as a collection of components, software component attributes identify the significant characteristics of the platform software. Platform software can be classified in terms of system services software (e.g., utilities, timers, diagnostics, configuration management), operating system (i.e., runtime executive), functional libraries (e.g., function blocks), and application software. The functional libraries and application software relate specifically to functionalities provided by the platform and are treated under the functionality attribute within this information class. Generally, this attribute category addresses the platform software itself and its performance characteristics. For example, the computer language is an attribute of the software itself and the execution approach relates to software performance. Complex logic for FPGAs and CPLDs are covered under this attribute category.

Software architecture: This attribute grouping involves the software elements of the platform, the relations among them, and the approach to executing system functions.

Runtime execution: This attribute grouping addresses the nature of the execution environment. Subattributes include task processing (e.g., sequential, timeslice sharing, parallel) and task scheduling (e.g., cyclic, interrupt driven). Determinism and real-time performance (e.g., response time, processing throughput) are key characteristics that should be captured.

Software (logic) complexity: This attribute corresponds to available metrics that characterize complexity. Complexity is added by design practices, many of which have been discouraged for safety-critical software (e.g., interrupt-driven processing, nondeterministic processing, state-dependent logic, dynamic memory allocation, shared memory).

COTS software components: This attribute indicates whether the platform software was developed specifically for nuclear safety usage, was dedicated for nuclear safety usage after initial commercial develop, or is general commercial-grade software.

Software languages: This attribute grouping can indicate the specific language(s) used by the platform or can identify the general category of software used, such as procedural (C), ladder (PLC), graphical, machine (assembly), hardwired logic (HDL), etc.

Software standards and design conventions: This attribute grouping identifies those standards adopted and design approaches employed in the development of platform software.

Fault tolerance: This attribute grouping identifies the self-testing and diagnostic software capabilities provided by the platform.

Software engineering tools: This attribute grouping identifies the design environment and other software tools employed by the platform vendor.

3.3.2.4 Human interfaces

Human interface attributes address the human-system interactions supported by the platform and the HMIs it provides. While, the HMI aspect of this attribute group could be treated as a subattribute within the hardware components or interconnections attribute categories, the human interface has special significance regarding its impact on human performance, which merits its treatment as a separate category.

Human factors standards: This attribute identifies the standards employed in developing and implementing human interfaces.

Displays: This attribute grouping addresses the types of display and indication provided by the platform. Examples of video display devices include cathode-ray tubes (CRTs) and flat panel displays (FPDs). Subattributes can include the style (e.g., textual or graphical) and the interactive capabilities (e.g., display-only, touch screen selection, click or push-button paging).

Input devices: This attribute grouping identifies the means for input and interaction provided by the platform (e.g., keyboards, mice, joysticks, trackballs, touch screen).

Dedication: This attribute identifies whether an HMI is dedicated to a specific system/function or interfaces with multiple systems. It can also be used to indicate the characteristics of interfaces. Examples include provision of spatially dedicated simple manual input devices (e.g., buttons, switches, keys) and displays (alarm tiles, recorders, indicator lights) and/or transferrable soft control interfaces with multiuse displays.

3.3.2.5 Interconnections

A DI&C system will generally have external connections to plant signals, electrical power, and communications links to other systems. Depending on the extent to which implementation details can be captured, these external connections can identified as data items within the system class as part of the

decomposition of the plant I&C architecture. The attributes of these interconnections can be hardware and software component attributes or functionality attributes. This category is not intended to duplicate attributes about the components or functionalities of a platform. Instead it is primarily focused on interdependencies with the connected external systems and interactions among significant internal elements (i.e., modules or components). For example, fault isolation on a communications network link is a specific instance of the communications characteristic attribute, robustness.

Communication interfaces: This attribute grouping relates to the hardware interface for each type of communications interconnection supported by the platform. Subattributes can include the transmission medium (backplane traces, copper cables, fiber optic cables, radio-frequency transmission), media access controllers (MACs) and hardware interconnects, and the topography of the communication link (e.g., point-to-point, serial bus, multinode network).

Interconnection independence: This attribute grouping addresses the means for providing electrical isolation for hardware interfaces and functional independence for communications interfaces. For example, electro-optical coupling may be used to provide electrical isolation. Buffering of the main (“safety”) processor from communications interactions through the use of a separate communications processor and interposing dual-port memory is an example of functional isolation.

Communications protocols: This attribute grouping involves identification of the approach to managing and executing communications. The highest-level attributes within this grouping can consist of identification of the standard or proprietary protocol by name. The nature of managing communication access among nodes (e.g., random shared access with collision detection/recovery, token passing, master/slave polling) should be indicated. The attribute grouping can be further subdivided to identify key characteristics of the syntax, semantics, and synchronization of the message transaction.

Communications characteristics: This attribute grouping addresses key characteristics of communications implementations that promote safety and reliability. These subattributes include determinism (e.g., scheduled, cyclic, fixed content), data flow (i.e., unidirectional or bidirectional messaging among nodes), addressing (e.g., peer-to-peer, broadcast), robustness (e.g., error detection, failure recovery, fault isolation), and security.

External power source: This attribute identifies the power needs of the platform (e.g., AC/DC, frequency, voltage, nominal power).

3.3.2.6 Quality

Quality attributes capture information about the quality assurance (QA) program that was (is) applied to design, manufacture, inspection, installation, testing, operation, and maintenance to ensure that the platform demonstrates quality commensurate with the importance of the plant functions to be performed. This attribute category is directly correlated to the safety classification associated with plant functions in the function class. Attributes within this category serve as indicators of the implementation and adherence to a QA program throughout the life cycle of a platform.

QA program: This attribute indicates whether a QA program was in place during the development and application of a platform.

Standards compliance: This attribute can expand to address a variety of safety standards from various organizations, with a breakdown of compliance with specific clauses/requirements, if the information is available.

Testing: This attribute grouping addresses the implementation of a testing program and the nature of the tests applied. Specific test types (e.g., unit testing, integrated testing, functional

testing) can be indicated along with the life cycle phase (if specified) at which the tests were applied.

Equipment qualification: This attribute captures characteristics of any equipment qualification (EQ) program applied to the platform. For example, the method of qualification (e.g., type test, analysis, operating experience), the tests employed (e.g., environmental, seismic, electromagnetic interference, surge withstand), and the nature of the EQ goal (e.g., compatibility with environmental extremes, aging for qualified life, exposure to accident conditions) are examples of subattributes.

Dependability: This attribute grouping involves characteristics of dependability, such as availability and reliability, as well as identification of the methods used to establish those dependability characteristics, such as PRAs, failure modes and effects analyses (FMEAs), software hazard analyses, requirements traceability analyses, etc.

Safety-grade certification: The data item for this attribute can consist of identification of any well-defined safety/quality certification, including certifications by international bodies (e.g., TÜV).

3.3.2.7 Functionality

Functionality attributes identify significant functional activities and actions that are performed by the platform. This attribute addresses the functionality provided by a platform that enables digital implementation of functions in current or planned installations. The platform functionality attributes can be associated with plant function attributes within the function class data set to relate application-specific system-level functions with the digital functionality provided by particular platforms. Implementation details can be captured in this manner if the information is available.

System-level functions: Examples of items in this attribute grouping include input/output processing, control, monitoring, voting, diagnostics, and communications.

Platform functionality: Examples of items in this attribute grouping include systems services (e.g., timers, resource access, configuration initialization), fault management, and function block libraries at higher-levels of information capture and functionalities such as acquisition, conversion, computation, comparison, limitation, storage, transmission, etc., at lower levels of information capture. [These attributes can be related to specific hardware components or software objects.]

4. CLASSIFICATION STRUCTURE APPLIED TO THE DI&C INVENTORY

This section describes the classification approach as it can be applied to the DI&C inventory developed based on this research. As described in Ref. 1, initial inventory data were gathered through data mining of available publications, reports, and information sources to identify existing DI&C systems from documentation of I&C modernization projects at domestic NPPs. The development of an initial inventory included a search of the principal repositories of OpE data for U.S. commercial NPPs—primarily data from the Equipment Performance and Information Exchange System (EPIX) that is maintained by the Institute of Nuclear Power Operation (INPO).

4.1 System Class Structure and Associations

The initial inventory data primarily consists of identification of the DI&C systems for individual units at specific plants. This data corresponds to an architectural view of the DI&C inventory and constitutes the topmost data items (or data objects) within the system class of the recommended classification framework. The highest level grouping of inventory data within this class is in terms of a DI&C system designation (i.e., name, type, or other identifier) by reactor unit at specific plants (e.g., Plant A Unit 1). As indicated in Sect. 3.1, the system designation can be categorized at a high level of abstraction (e.g., NSSS safety system, BOP nonsafety system, etc.) or resolved into types based on generic plant I&C architectures and the specific DI&C system name assigned by the plant. Figure 10 conceptually illustrates the collection of data items within the DI&C inventory for the system class. For each object of the system class, the principal data consists of the DI&C system name (or type) coupled with other attributes (or system identification properties) that can include service dates (e.g., date of installation, service life), high-level identification of the digital platform used for the implementation, plant function performed, and system architecture (e.g., configuration and interconnections), as available.

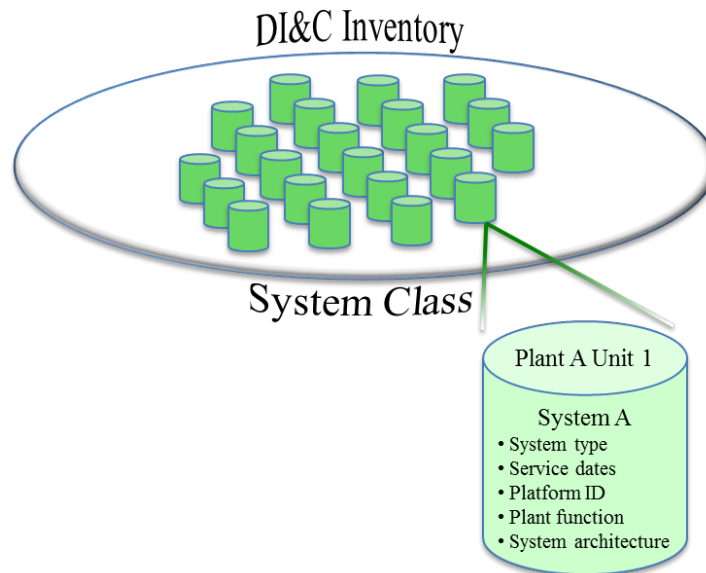


Fig. 10. DI&C inventory data objects for the system class.

4.2 Decomposition of System Class

System architecture information provides the direct connection for the data objects in the inventory to the actual organization of the systems in the plant. This relationship is established through decomposition of the I&C architecture of a plant into a whole-part representation of the I&C systems. As previously discussed, each DI&C system involves the primary computational machine, inputs, outputs, human interfaces, and (potentially) interconnections with other I&C systems. Each element within this structural representation can be decomposed into subelements (e.g., subsystems, modules, components). Figure 11 illustrates an approach to system decomposition within this classification framework. At each layer of the decomposed whole-part representation, data objects corresponding to subclasses within the system class framework can be established to capture knowledge about subelements (e.g., physical components, software objects) at lower levels of the system architecture. Obviously, the lowest levels of the system architecture correspond to the basic components and internal configuration of the digital platform itself. The depth to which this data class can be populated is heavily dependent on the availability of detailed information on specific implementations.

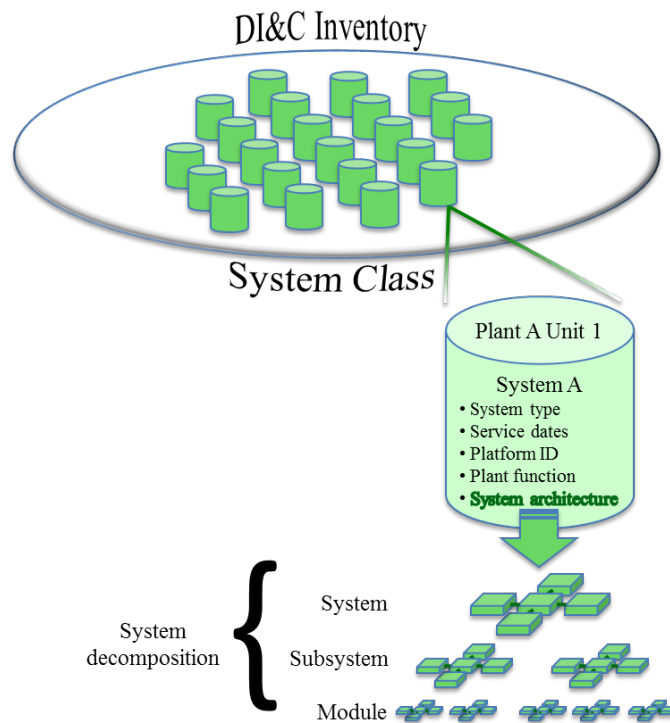


Fig. 11. Hierarchical data decomposition within the system class.

4.3 Function Class Structure and Associations

The plant functions performed by specific DI&C systems were not typically reported by most of the information sources investigated during this research. However, when available, the designation of the plant function performed by a DI&C system can be incorporated as a data attribute within the system class. This data attribute can serve as an indication of the purpose and significance of each DI&C system as well as provide a means to establish a link with more detailed information about the allocation of function to digital technology.

As the DI&C inventory evolves, more detailed targeted analyses of the available knowledge base can be conducted to capture information about which plant functions are assigned to a DI&C system. As

observed in Sect. 3.2, information about plant functions can be derived from knowledge of plant designs and typical I&C architectures, safety evaluation and licensee event reports, and system functional requirements and safety classification. Data about the implementation of plant functions in DI&C systems corresponds to a functional view of the DI&C inventory and the designation of each digitized function constitutes the topmost data items within the function class of the recommended classification framework.

Figure 12 depicts the collection of data items within the DI&C inventory for the function class. For each item of the Function Class, the principal data consists of the purpose and safety classification for each plant function. Safety classification for high-level plant functions is well defined and can be easily captured. The purpose of a plant function generally must be extracted by analysis from information sources, such as those identified above. Where available, each data object within the function class can include a representation of the allocation of function within the system architecture and the application of digital functionality that implements the plant function. The primary value of the functionality attribute is to capture what functional elements (e.g., subfunctions, algorithms, tasks) are implement using digital technology and what digital functionality is critical to enable execution of the primary function of a system. However, detailed knowledge of an actual implementation is necessary to provide more than a high-level listing of generic functionality that is likely to be required to support any particular plant function. Thus, this data attribute is highly implementation specific and is most relevant in the context of an analysis of the impact and significance of critical characteristics for specific applications on particular digital platforms.

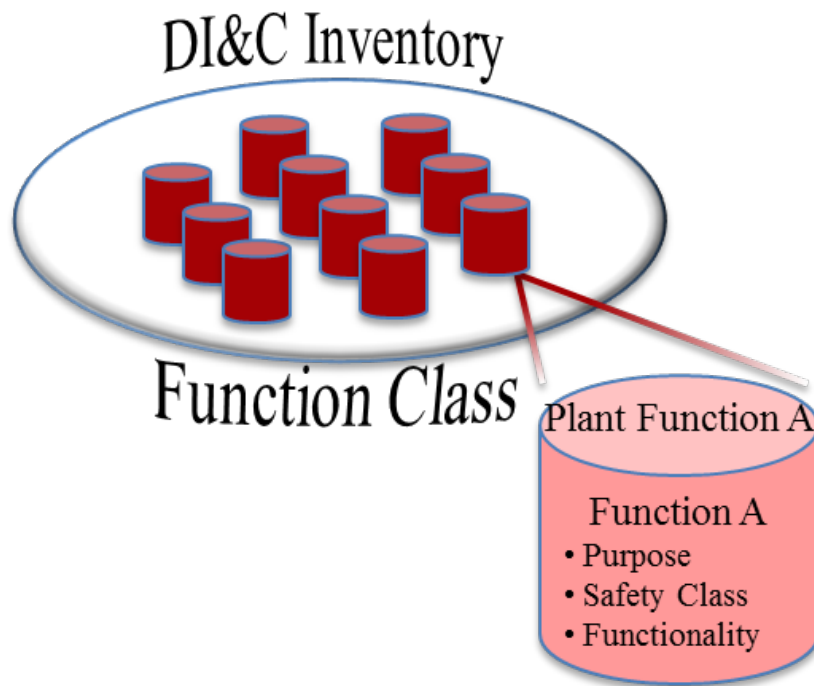


Fig. 12. DI&C inventory data objects for the function class.

As previously noted, the highest level of abstraction for the attribute corresponding to the purpose of the plant function involves functional groupings in terms of protection, control, and monitoring. More distinct groupings can be characterized in terms of typical subdivisions of plant I&C architectures, such as measurement, automatic regulation (i.e., control), safety/protection, monitoring, communications, display and manual control, actuation, etc. Adopting a whole-part representation approach, these functional groupings can be further decomposed into specific plant functions such as those listed in Appendix B.

4.4 Linking System and Function Classes

The data objects within the function class are linked to the data objects within the system class through the plant function attribute of the system class. Basically, the identification of plant function allocated to a specific DI&C system in the system class is associated with the designation of particular functions (in terms of functional groupings) at the highest-level of the function class data hierarchy. Figure 13 illustrates the connection among the data objects in the different classes. The double-ended arrow between the generic data objects in the figure represents the data association between the plant function attribute for the System A object and the Function A object. In addition, as the level of detail increases in the representation of the purpose attribute of the function class (i.e., finer granularity in the decomposition of the functional groupings representing the purpose of plant functions), the connection with subelements (e.g., modules, components) of a DI&C system becomes apparent and the associations can be extended to lower layers within the system class structure.

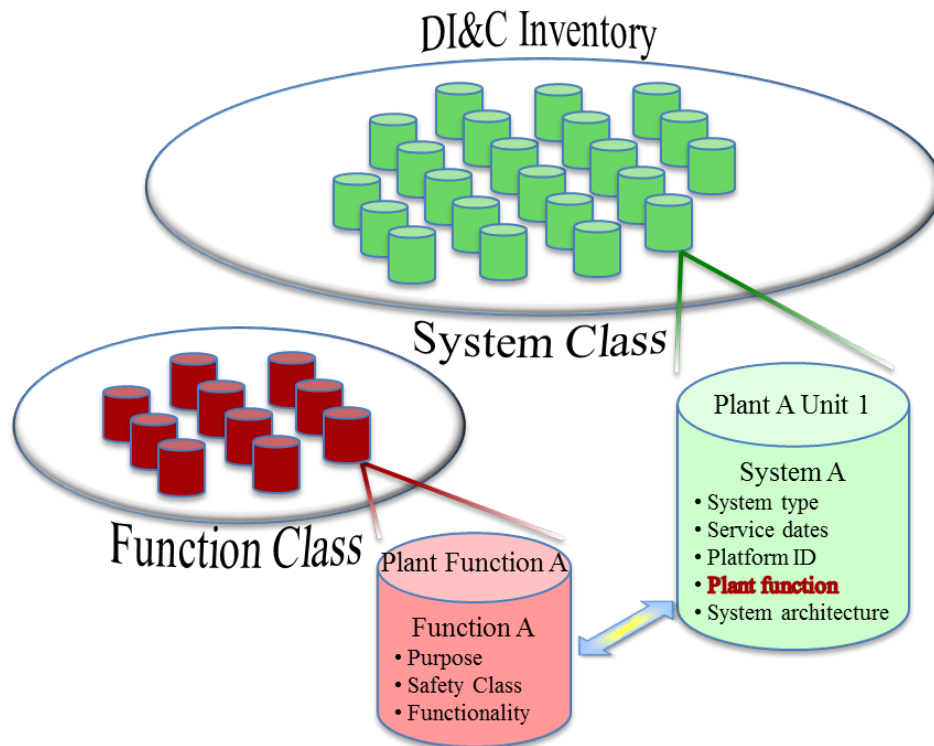


Fig. 13. Data association between system and function classes.

4.5 Platform Class Structure and Associations

The initial inventory data also includes high-level identification of the digital platform employed to implement each DI&C system. Generally, this information involved identification of the system supplier and product name, with model number and/or version occasionally noted. Most information sources did not provide extensive information about the platform components, capabilities, and configuration. However, as described in Sect. 3.3.1, other sources of platform information were investigated to identify what type of data could be collected. Such data corresponds to a technological view of the DI&C inventory. Data sets corresponding to individual platforms constitute the topmost data objects within the platform class of the recommended classification framework. These platform-specific data sets consist of information about critical (e.g., design and performance) characteristics that can be extracted from supplier information, technical reports, and design evaluations. Because of the unique nature of each platform and the prospective need to protect sensitive information, the data sets could be treated as

individual databases that collectively represent a compound database of platform designs. Figure 14 illustrates the collection of platform data sets and a representative data object within the DI&C inventory for the platform class.

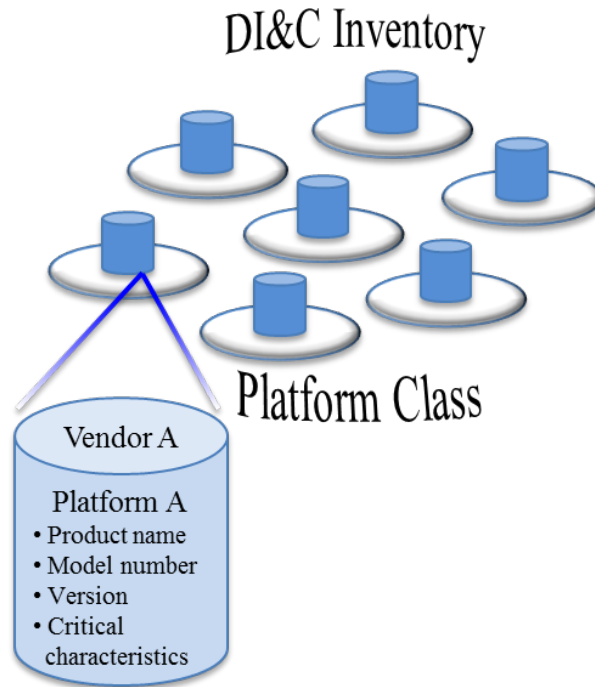


Fig. 14. DI&C inventory data sets and data object for the platform class.

4.6 Linking System and Platform Classes

Figure 15 depicts the connection between a platform-specific data set and the principal data within the DI&C inventory. The double-ended arrow between the generic data objects in the figure represents the data association between the platform ID attribute for the System A object and the Platform A data set. Specifically, the platform ID attribute relates to the vendor and platform identifiers (e.g., product name, model number, and version) corresponding to the particular platform represented by the data set.

The specific attribute categories described in Sect. 3.3.2 identify the types of information that can be captured in each data set. These attributes provide the means for identifying platforms with common features or characteristics and can be used to selectively screen the platforms according to features of interest. For example, the interconnections attribute category includes communications protocols as a specific data attribute. A data query of each platform data set can identify those platforms that use a specific protocol of interest. Based on those search results, a data query of the system class data objects can identify what systems at which plants are based on the platforms that have been found to use the protocol of interest. Thus, the instances of a particular communications protocol in the installed base of DI&C systems can be determined and this knowledge can contribute to an analysis of OpE information. Similar searches can be conducted for various features and characteristics of digital technology depending on the level of detail captured for each platform that is included in the inventory and collated under the platform class.

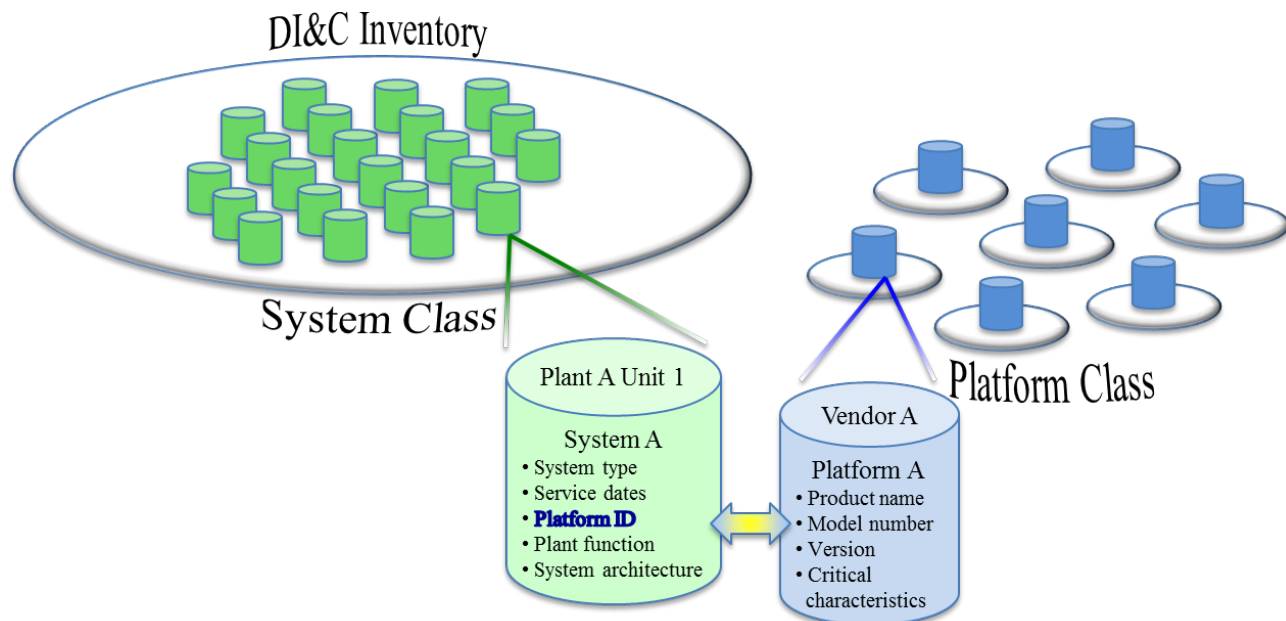


Fig. 15. Data association between system and platform classes.

Platform configuration attributes (e.g., architecture, hardware components, software components, human interfaces, interconnections) also serve to provide links with the lower level subclasses of the system class (see Fig. 16, where the double-ended arrow represents the data association between attributes of the two classes). Effectively, the lowest levels of system decomposition (e.g., module, component) within the system class correspond to the platform architecture and component attributes of the platform class. Thus, there is a direct association between the key data items within the system and platform classes as the representation of actual systems becomes more finely resolved.

The relationship between the data contained in the system class and that of the platform class can be further illustrated based on a simplified decomposition of a plant I&C architecture (see Fig. 17). In this example, the plant I&C architecture consists of three representative DI&C systems. The first system type corresponds to a control system (e.g., turbine or feedwater control system), the second system type corresponds to a safety system, and the third system type corresponds to a monitoring system. The safety system of this example is implemented as two diverse subsystems. Each endpoint in the decomposition of the plant I&C architecture corresponds to an application-specific implementation of a digital platform. Thus, System 1 represents a control system based on Platform A (e.g., TRICON). System 3 represents a monitoring system based on Platform C (e.g., Intelligent Automation I/A Series). System 2 is further decomposed into Subsystem 1 based on Platform A (e.g., TRICON) and Subsystem 2 based on Platform B (e.g., Spec 200 Micro). The system class data sets contain identification of the platform in each case, along with any application-specific information (e.g., interconnections to other I&C systems in the plant, details of the application software, unique hardware configurations), while the platform class data sets contain basic information about the platform itself (e.g., internal architecture, critical characteristics). Thus, as illustrated in the figure, the lowest information levels of the system decomposition hierarchy in the system class relate directly to the more detail information embodied for each applied platform in the platform class.

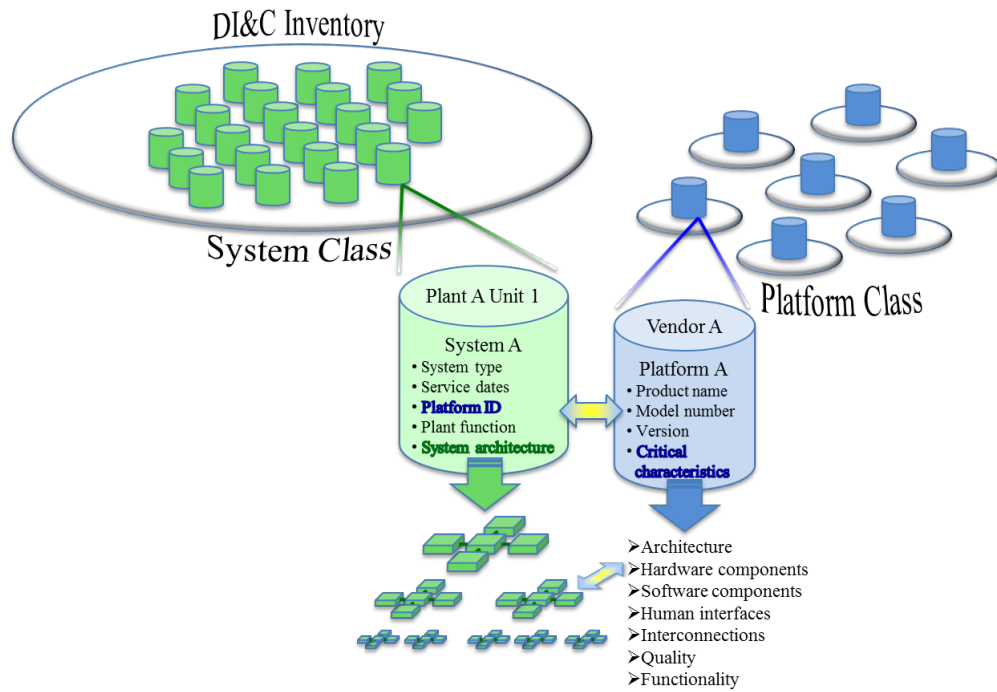


Fig. 16. Extended data associations between system and platform classes.

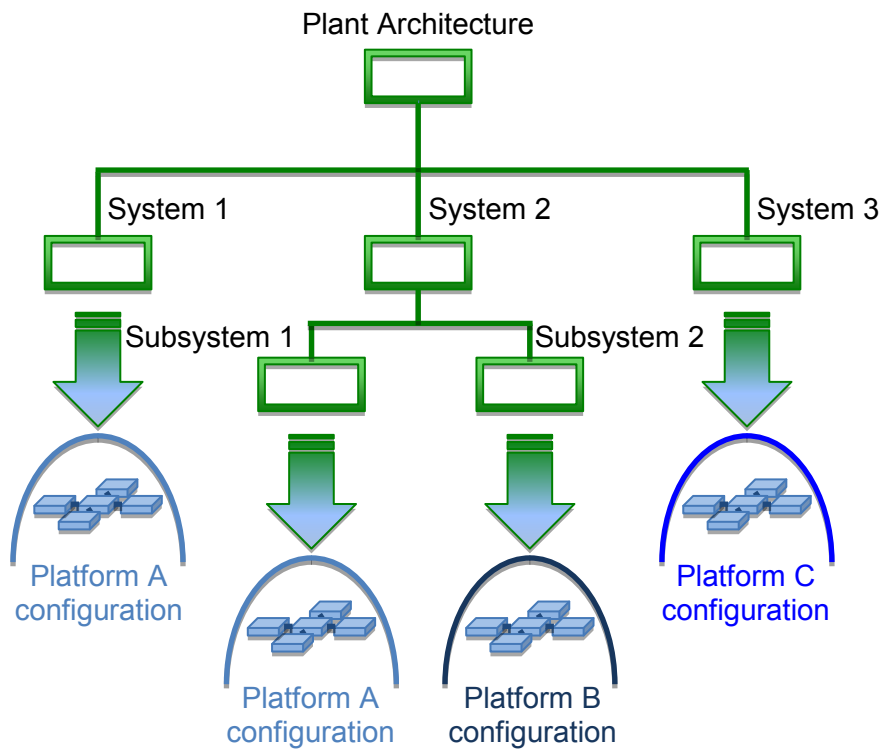


Fig. 17. Simplified decomposition illustrating relationship between system and platform classes.

4.7 Linking Platform and Function Classes

The functionality attribute category provides the means for relating data within the platform class to data within the function class. In particular, the digital functionality provided by a platform serves as the basis for implementing plant functions as part of a specific application. As noted above in the discussion of the function class structure, the critical characteristics for specific applications on particular digital platforms establish a context for decomposing plant functions into digital functionality. In practice, the relationship between basic functionality of the platform and plant functions implemented on the DI&C system is more readily established from a bottoms-up perspective, which essentially captures the building of system-level functions from platform-specific capabilities as is the case in the design and implementation lifecycle phases for a particular application. Figure 18 illustrates the association between the functionality attribute of a platform data set and the decomposed functionality at the lower levels of a function class data object. The double-ended arrow denotes the data association while the arrows representing the expansion of the data attributes shows the top-down approach to resolving the data with finer granularity for both classes as well as a bottoms-up approach for relating the more fundamental representation of digital functionality to the higher-level abstraction of functional groupings for the function class. As noted, this relationship is highly implementation specific and detailed information may be difficult to acquire. Thus, incorporating this level of detail into the inventory may be best treated initially on an as-needed basis to support specific analyses.

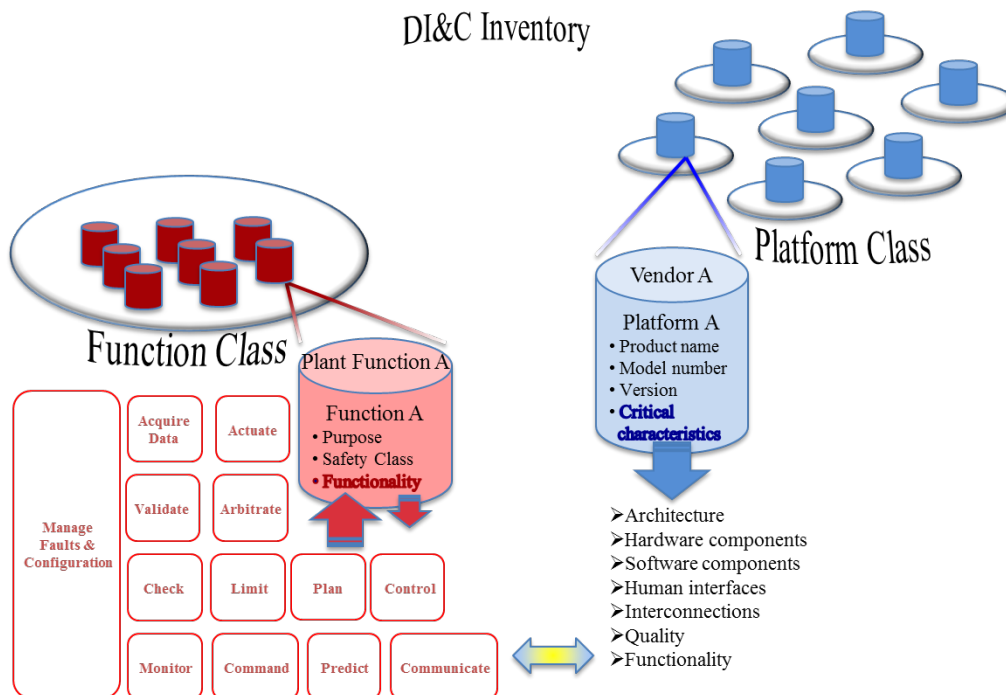


Fig. 18. Elementary data association between function and platform classes.

4.8 Fully Integrated DI&C Classification Structure

Figure 19 depicts the classification structure as a whole. As described above, the data objects and data sets within each class constitute the total collection of information to establish a fully realized DI&C inventory. The recommended classification structure provides an approach to organizing the DI&C inventory data that has been acquired thus far while providing a flexible framework to accommodate the

additional data that is most likely to be available through future investigations. By establishing the higher-level data categories within each class, this classification structure identifies the basic information that should be captured. The hierarchical nature of the data collection, in terms of high-level abstractions of key attributes that decompose into lower level, more finely resolved representations, is illustrated for each information class. This organizational approach enables inclusion of more detailed data and expansion of information categories to be pursued as the DI&C inventory evolves. In addition, the data associations among attributes for the three information classes are also indicated in the figure. This data collection can be implemented as a monolithic database or within subordinate databases that are interconnected through metadata associations that support relational searches. Based on these associations, specific functions, features, and/or characteristics can be selected for searches to identify commonalities among DI&C systems and enable groupings by properties of interest. This capability can be used to support in-depth investigations of the impact of digital technology, which can include assessments of performance or failure experience and analyses of common cause failure vulnerabilities.

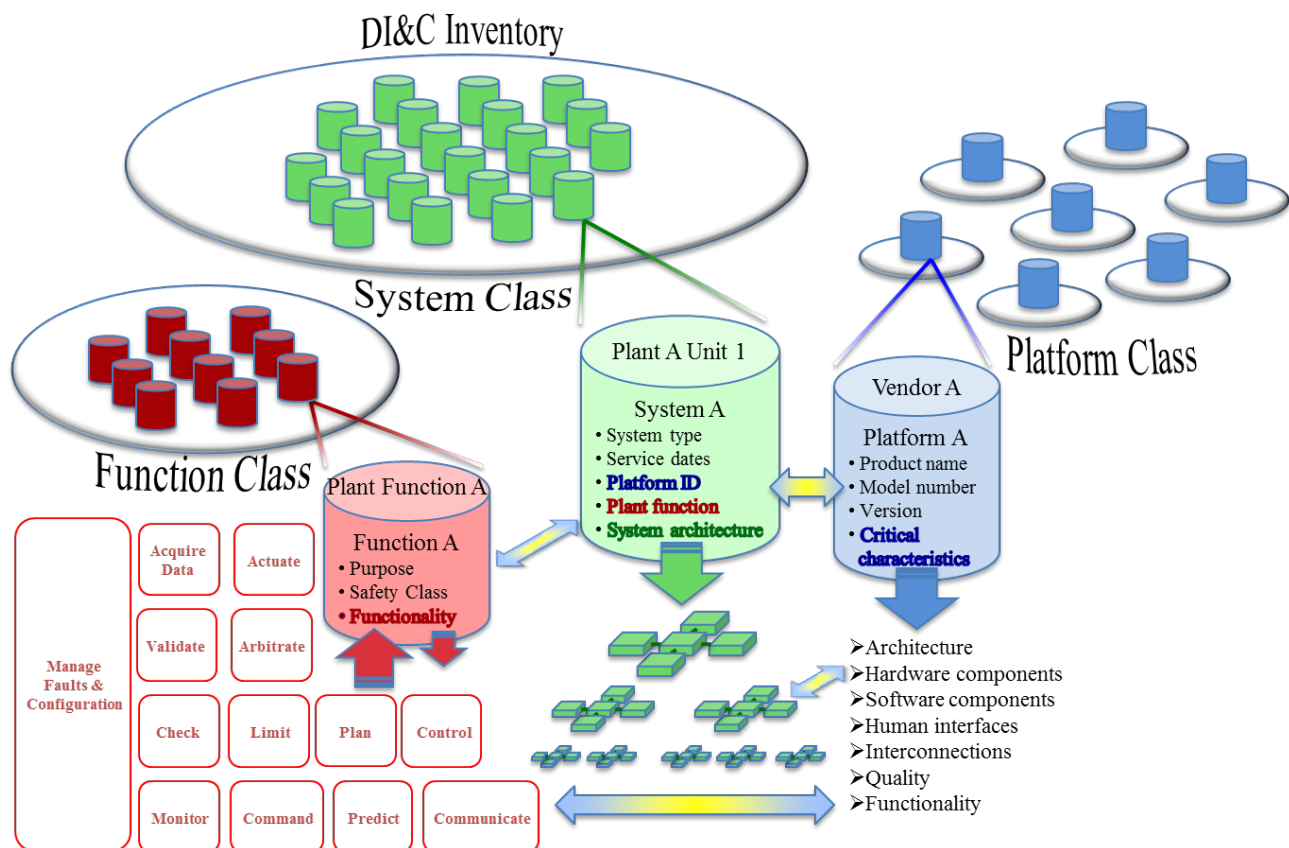


Fig. 19. Overall classification structure for DI&C inventory.

Page intentionally blank

5. CONCLUSIONS

The commercial I&C marketplace is dominated by digital technology designed to serve the needs of nonnuclear industries, which demand the advanced capabilities and features it supports. With the increasing obsolescence of existing analog-based I&C technology and the desire to achieve enhanced performance and some reliability improvements, the nuclear power industry is modernizing the I&C systems at the plants. Consequently, the extent of digital technology usage at U.S. nuclear power plants is expanding. New plants will employ digital technology in safety and nonsafety systems extensively. Therefore, the nuclear power industry stakeholders and NRC staff must have confidence in the safety-relevant characteristics of this equipment to enable effective and efficient licensing and implementation.

This research activity contributes to the development of the needed level of confidence by identifying the extent and nature of DI&C systems in nuclear power plants to form the basis for an initial inventory. Knowledge of the penetration of digital technology into the U.S. nuclear industry establishes a better defined context for the review of operating experience and performance characteristics regarding DI&C systems, which then facilitates informed consideration of best practices, lessons learned, and favorable performance that may not be adequately captured in current OpE databases.

The investigation of classification approaches found that information is typically organized based on one or more of four primary approaches:

- safety significance,
- physical representation,
- functional representation, or
- critical characteristics.

Based on the evaluation of these classification approaches, it was determined that no single approach among those investigated was suitable to be directly adopted in organizing the DI&C inventory information. Consequently, ORNL developed recommendations on a classification structure that is based on relevant structural elements drawn, to varying degrees, from the approaches that were evaluated. The development of the recommendations was driven by project expectations that the classification approach must (1) meet NRC system analysis needs, (2) provide a suitable structure for organizing the inventory information, and (3) be sufficiently flexible to support the subsequent introduction of expanded categories and additional information as the inventory evolves.

The focus of the recommended classification approach centers on three key elements:

- a system class (essentially the inventory data set reported in Ref. 1) that adopts a system architectural structure to provide categorization by system, subsystem, module, component, etc., for DI&C systems;
- a function class that describes plant functions (e.g., protection, control, and monitoring) and the related digital functionality as it is implemented in DI&C systems while indicating the significance of the function based on existing safety classification; and
- a digital platform class derived principally from an investigation of SERs for previously approved DI&C platforms (e.g., TRICON, Common Q, Teleperm XS) in which a number of key platform attributes are identified to provide the basis for characterizing each platform in terms of critical features.

By establishing data associations among the categories, the classification structure can enable DI&C inventory information to be related to critical characteristics identified through digital platform features and safety significance associated with plant function. Further expansion of the classification structure

can allow operating experience data to be incorporated in the relational structure to support system analyses by NRC.

The classification structure developed under this research effort provides a framework and structure for establishing the initial set of key relationships among the three classes—System, Function, and Platform—that not only supports the “characterization” of DI&C systems but also provides the foundation for later development of a relational database and/or information system to readily search detailed information on DI&C systems.

6. REFERENCES

1. W. P. Poore III et al., *Initial Inventory of Digital I&C Systems Used in Domestic Nuclear Power Plants*, LTR/NRC/RES/2012-002, Oak Ridge National Laboratory, January 2012. [NRC Agencywide Documents Access and Management System (ADAMS) Accession Number [ML120410275 Proprietary Information Non-publicly Available](#)].
2. U.S. Nuclear Regulatory Commission, *U.S. Code of Federal Regulations*, Title 10, Part 50, “Domestic Licensing of Production and Utilization Facilities,” Washington, DC.
3. Institute of Electrical and Electronics Engineers, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” IEEE Std. 323-2003, Piscataway, New Jersey, 2003.
4. International Atomic Energy Agency, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*, IAEA NS-G-1.3, Vienna, Austria, 2002.
5. International Electrotechnical Commission, *Nuclear Power Plants—Instrumentation and Control for Systems Important to Safety—General Requirements for Systems*, IEC 61513, Geneva, Switzerland, March 2001.
6. International Electrotechnical Commission, *Nuclear Power Plants—Instrumentation and Control Systems Important for Safety—Classification*,” ed. 2.0, IEC 61226, Geneva, Switzerland, February 2005.
7. International Atomic Energy Agency, *Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants: A Reference Book*, Nuclear Energy Series Report, IAEA NP-T-3.12, Vienna, Austria, December 2011.
8. Don Dudenhoeffer et al., *Technology Roadmap: Instrumentation, Control, and Human Machine Interface to Support DOE Advanced Nuclear Power Plant Programs*, INL/EXT-06-11862, Idaho National Laboratory, Idaho Falls, Idaho, March 2007.
9. John O’Hara, Bill Gunther, and Gerardo Martinez-Guridi, *The Effects of Degraded Digital Instrumentation and Control Systems on Human-System Interfaces and Operator Performance: HFE Review Guidance and Technical Basis*, BNL-91047-2010, Brookhaven National Laboratory, Upton, New York, February 2010.
10. W. P. Poore III et al., *Sequence Coding and Search System Quality Assurance Program*, ORNL/NOAC-225, Rev. 3, Oak Ridge National Laboratory, Oak Ridge, Tennessee, September 1991.
11. Electric Power Research Institute, *Programmable Logic Controller Qualification Guidelines for Nuclear Applications, Volume 1*, EPRI TR-103699, Vol. 1, October 1994.
12. Electric Power Research Institute, *Programmable Logic Controller Qualification Guidelines for Nuclear Applications, Volume 2*, EPRI TR-103699, Vol. 2, October 1994.
13. Electric Power Research Institute, *Programmable Logic Controller Qualification Guidelines for Nuclear Applications, Volume 2*, EPRI TR-103699, Vol. 2, October 1994.
14. J. Rasmussen, *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering*, Elsevier Science Inc., New York, 1986.
15. J. Rasmussen et al., *Cognitive Systems Engineering*, John Wiley & Sons, New York, 1994.
16. G. Weinberg, *An Introduction to General Systems Thinking*, John Wiley & Sons, New York, 1975.

17. N. Leveson, "A New Accident Model for Engineering Safer Systems," *Safety Science*, **42**(4), pp. 237–270 (2004).
18. J. C. Laprie, "Dependable Computing: Concepts, Limits Challenges," *Proceedings of the 25th IEEE International Symposium on Fault-Tolerant Computing—Special Issue*, Institute of Electrical and Electronics Engineers, Pasadena, California, pp. 42–54 (1995).
19. J. H. Lala and R. E. Harper, "Architectural Principles for Safety-Critical Real-Time Applications," *Proceedings of the IEEE*, **82**(1), pp. 25–40 (1994).
20. M. J. Hawthorne and D. E. Perry, "Applying Design Diversity to Aspects of System Architectures and Deployment Configurations to Enhance System Dependability," in *Proceedings of the International Conference on Dependable Systems and Networks*, Institute of Electrical and Electronics Engineers, Florence, Italy, June 2004.
21. Electric Power Research Institute, *Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems*, EPRI TR-1016731, Palo Alto, California, December 2008.
22. U.S. Nuclear Regulatory Commission, *Common-Cause Failure Database and Analysis System: Event Definition and Classification, Vol. 2*, NUREG/CR-6268, Washington, DC, June 1998.
23. U.S. Nuclear Regulatory Commission, "Assessment of Digital System Operating Experience Data and System Inventory and Classification Structure," unnumbered memorandum, Washington, DC, March 2008 [NRC Agencywide Documents Access and Management System (ADAMS) Accession Number ML080590323].
24. S. A. Arndt, "Development of Regulatory Guidance for Risk-Informing Digital System Reviews," *5th International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technology (NPIC & HMIT 2006)*, American Nuclear Society, Albuquerque, New Mexico, November 2006.
25. J. Rushby, "Critical System Properties: Survey and Taxonomy," *Reliability Engineering and System Safety*, **43**, pp. 189–219 (1994).
26. C. Perrow, *Normal Accidents: Living with High Risk Technologies*, Basic Books, New York, 1984.
27. U.S. Nuclear Regulatory Commission, *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments*, NUREG/CR-6901, Washington, D.C., February 2006.
28. Stuart Richards, U.S. Nuclear Regulatory Commission, letter to James Mallay, Siemens Power Company, "Acceptance for Referencing of Licensing Topical Report EMF-2110(NP), Revision 1, 'Teleperm XS: A Digital Reactor Protection System' (TAC NO. MA1983)," May 5, 2000 (ADAMS Accession No. ML003711856).
29. Stuart Richards, U.S. Nuclear Regulatory Commission, letter to Philip Richardson, Westinghouse Electric Company, "Acceptance for Referencing of Topical Report CENPD-396-P, Rev. 01, 'Common Qualified Platform,' and Appendices 1, 2, 3, and 4, Rev. 01 (TAC NO. MA1677)," August 11, 2000 (ADAMS Accession No. ML003740165).
30. Stuart Richards, U.S. Nuclear Regulatory Commission, letter to Troy Martel, Triconex Corporation, "Review of Triconex Corporation Topical Reports 7286-545, 'Qualification Summary Report' and 7286-546, 'Amendment 1 to Qualification Summary Report,' Revision 1 (TAC NO. MA8283)," December 11, 2001 (ADAMS Accession No. ML013470433).

APPENDIX A. GENERIC SYSTEMS FOR BWR AND PWR DESIGNS

Page intentionally blank

APPENDIX A

Table A.1. Catalog of generic systems for a BWR design

Generic BWR Systems
Area Radiation Monitoring System
Automatic Depressurization System
Core Spray System
Diesel Generator Control
Electro-Hydraulic Control System
Feedwater Control System
Fire Protection System
Fuel Pool Cooling and Cleanup System
High Pressure Coolant Injection System (HPCI)
High Pressure Core Spray System
Makeup Water Control System
Plant Service Water System
Post-Accident Sampling System (PASS)
Power Range Neutron Monitoring System
Primary Containment Isolation System
Process Radiation Monitoring System
Reactor Core Isolation Cooling System
Reactor Protection System
Reactor Recirculation Control System
Reactor Water Cleanup System
Redundant Reactivity Control System
Remote Shutdown System
Residual Heat Removal System
Rod Control & Information System
Rod Sequence Control System
Rod Worth Minimizer
Standby Gas Treatment System
Standby Liquid Control System
Startup Range Neutron Monitoring System (SURNMS)
Steam Bypass and Pressure Regulating System (SB&PR)
Steam Leak Detection System
Traversing Incore Probe System (TIP)

Table A.2. Catalog of generic systems for a PWR design

Generic PWR Systems
Area Radiation Monitoring System
Auxiliary Feedwater Control System
Chemical and Volume Control System
Component Cooling Water Control System
Condensate and Feedwater Control System
Condensate Cleanup Control System
Core Protection Calculator
Diesel Generator Control System
Engineering Safety Features Actuation System
Ex-core Nuclear Instrumentation System
Heating, Ventilation, and Air-Conditioning System
Integrated Control System
Loose Parts Monitoring System
Main Feedwater Control System
Main Feedwater Pump Control System
Post-Accident Monitoring System
Pressurizer Level Control System
Pressurizer Pressure Control System
Process Radiation Monitoring
Reactor Makeup Control System
Reactor Protection System
Rod Control System
Rod Position Indication System
Service Cooling Water Control System
Steam Dump Control System
Steam Generator Blowdown Processing System
Steam Generator Level Control System
Turbine Electro-Hydraulic Control System

APPENDIX B. PLANT FUNCTIONS FOR A PWR DESIGN

Page intentionally blank

APPENDIX B

Table B.1. Catalog of plant functions for a PWR design

PWR Functions
Pressurizer Level Control/Protection
Pressurizer Pressure Control/Protection
Reactor Coolant Low Flow Protection
Turbine Impulse Chamber Pressure Protection
Containment Pressure Protection
Reactor Coolant Wide Range Temperature Control/Protection
Reactor Coolant Wide Range Pressure Control/Protection
Steam Generator Level Protection and Feedwater Control
Refueling Water Storage Tank Level Protection
Containment Sump Level Protection
Steam Flow and Feedwater Flow Protection
Steam Pressure Control/Protection
Average and Delta Temperature Protection
Condensate Storage Tank Level Protection
Pressurizer Liquid and Vapor Temperature Protection
Reactor Vessel Level Instrumentation
Reactor Protection Logic
Engineering Safety Features Logic
Boric Acid Tank Level
Residual Heat Removal Pump Discharge Temperature
Rod Control
Steam Dump Control
Volume Control Tank Level Control
Boric Acid Blend Control
Radiation Monitoring
Rod Position Indication
Flux Mapping
NSCW Pumps, Pressure Interlock
Reactor Make-Up Pump, Flow Interlock
Diesel Storage Tanks, Pressure Interlock
DG, Diesel Fuel Oil Storage Tanks Level Indication
Containment Wide Range Pressure Monitor
Nuclear Service Cooling Water (NSCW) Cooling Tower, Spray Header Bypass Valve Control
Condensate Storage Tanks, Level Monitor
NSCW Engineered Safety Features (ESF), Water Chiller Flow
Auxiliary Feedwater to Steam Generators, Flow
Auxiliary Feedwater Pumps, Mini Flow Control
Component Cooling Water (CCW) Pumps, Header Pressure Interlock
Auxiliary Feedwater Pump, Turbine Speed Control
Turbine Trip – Reactor Trip – Control Valves Hydraulic Pressure
Auxiliary CCW (ACCW) Pumps, Header Pressure Interlock
NSCW Cooling Tower, Fan Temperature Control
Reactor Coolant Pump (RCP) Thermal Barrier Heater, Return Header
RCP Thermal Barrier Heater, ACCW Outlet Flow
Piping Penetration Area Pressure
Diesel Generator (DG) Electrical Penetration Area Pressure
DG Power Output, Trains A & B

Table B.2. Catalog of plant functions for a PWR design (continued)

PWR Functions
Main Steam Atmosphere Relief, Loops 1-4, Pressure
Steam Generator's Blowdown, Pipe Break Room Protection, Flow
Steam Generator's Blowdown, Pipe Break Room Protection, Temperature
Chemical and Volume Control System (CVCS) Letdown, Pipe Break Room Protection, Pressure
CVCS Letdown, Pipe Break Room Protection, Temperature
Electric Steam Boiler, Flow
Electric Steam Boiler, Pipe Break Room Protection, Temperature
Containment (CT) Emergency Sump Level Monitor
Condenser Hotwell Level Control
Condenser Pump Discharge Header Pressure Indication
Condensate Steam Jet Air Ejector (SJAE) Minimum Flow Control
Condenser Header to Steam Generator Feedwater Pump Turbine's (FPT's) Pressure Indication
Feedwater Start-Up Recirculation Flow Control
Heater Drain, Pump's Discharge Pressure
Auxiliary Feed Pump, Turbine Impulse Pressure
Turbine Driven, Auxiliary Feedwater Pump, Discharge Pressure Monitor
Turbine Driven, Auxiliary Feedwater
Moisture Separator, Drain Tanks Level Indication
Auxiliary Feedwater Isolation Valves, to Steam Generators, Position
Motor Driven, Auxiliary Feedwater Pump, Discharge Pressure Monitor
CCW, Supply Header Pressure
CCW Pumps Discharge Header Flow
NSCW Reactor Cavity & Control Rod Drive Mechanism (CRDM) Cooling Coils Flow
Steam Generator Feed Pumps, Minimum Flow Control
Feedwater Heater Condensate Discharge Temperature
Steam Generator Feed Pumps Discharge Pressure
Steam Generator FPT's Speed Monitor
Steam Generator FPT's Bearing Oil Temperature Control
Steam Generator FPT's Hydraulic & Bearing Oil Pressure
Auxiliary Steam Blanketing to Moisture Separator Reheater's (MSR's), Pressure Control
Reheater's Heating Steam Supply Pressure Monitor
Reheater's Heating Supply Temperature Monitor
Steam Packing Exhauster Suction Pressure
Reheater's Heating Steam Supply Flow Monitor
Feedwater Heater Shell Level Indication
Main Steam to Control Valve
Steam Seal Header, Generator Hydrogen, & Condenser Water in Pressure Monitors
Reheat Steam to Low Pressure (LP) Turbines, Pressure Monitor
Main Steam to Stop Valves, Temperature Monitor
High Pressure Turbine (HPT) Exhaust to MSR, Pressure Monitor
Intermediate Steam, Pressure Monitor
LP Turbine Exhaust Hood's, Pressure Monitor
Turbine Bearing Oil Header & Hydraulic Fluid, Pressures Monitor
Turbine Lube Oil Cooler Discharge Temperature Control
Steam Generator FPT's Feedwater Demand Signal & SMF Input

Table B.3. Catalog of plant functions for a PWR design (continued)

PWR Functions
Turbine Plant, Cooling Water Pumps Discharge & Closed Cooling Water Supply, Temperature Indications
Turbine Plant, Closed Cooling Water Pumps Discharge & Cooling Tower Pumps Discharge Header, Pressure Monitors
Turbine Plant, Cooling Water Pumps Discharge Flow Indication
Generator Hydraulic Coolers Temperature Control
Condenser Inlet-Circulating Water Header, and Condenser Pumps Discharge Header, Temperature Monitors
Steam Generator FPT's Mode Transfer Comparator Deviation Inhibit
Circulating Water, Pump Basis & Canal, Level Monitors & Alarms
River Make-Up Water, Cooling Tower Blowdown, & Waste Water Retention Basin Discharge Flows
Turbine Plant Closed Cooling Water Make-Up Surge, Demineralized Water, & Reactor Make-Up Water Storage, Tanks Level
Steam Generator Blowdown Flow Setpoint
Electro-Hydraulic controller (EHC) Fluid Storage Tank Temperature Control
CCW & ACCW Surge Tanks Level Alarms
Waste Water Effluent Sulfonator Flow
Nuclear Service Cooling Tower Return Header Temperature Monitor
Nuclear Service Cooling Tower Leak Detection
NSCW for Containment Coolers' Flow
Instrument Air & Service Air Header's Pressure Monitor
NSCW Cooling Towers Supply & Return Flows
Cooling Tower Blowdown Conductivity Controller
NSCW for Diesel Generators' Flow Alarms
NSCW Cooling Tower Basin's Level Monitor
Main Steam to Stop Valves 1 & 2, 3 & 4 Pressures Indication
Main Steam & Hot Reheat Steam to Steam Generator FPT's Pressures Indication
Feedwater Heater's Discharge Temperature Controls
Feedwater Heater's Shell Pressures Monitor
Feedwater Heater Drain Pump's Net Positive Suction Head (NPSH) Controls
Containment Emergency Sump Temperature Indications
Heaters and Reheaters Drain Tanks Level Indications
Steam Generator Feedwater & Auxiliary Feedwater Inlet Temperature Indication and Alarms
Auxiliary Feedwater Pump Turbine Steam Flow Indication
Condensate Flow for Chemical Injection Control Monitor
Control Room Pressure Differential Control
Auxiliary Building Pressure Differential Control

Page intentionally blank

**APPENDIX C. ATTRIBUTE CATEGORIES FOR THE INFORMATION STRUCTURE
OF THE PLATFORM CLASS**

Page intentionally blank

APPENDIX C

Table C.1. Attribute categories for the information structure of the platform class

Principal Attribute Categories	Attributes within Category
Architecture	Physical arrangement
	Configuration management
	Fault management strategies
	Watchdog timer protection
	Maintainability
Hardware components	Types of modules/components
	Technology basis
	Digital processor identification
	On-board identification
	Nuclear-grade or COTS components
	Environmental rating
Software components	Software architecture
	Runtime execution
	Software (logic) complexity
	COTS software components
	Software languages
	Software standards and design conventions
	Fault tolerance
	Software engineering tools
Human interfaces	Human factors standards
	Displays
	Input devices
	Dedication
Interconnections	Communication interfaces
	Interconnection independence
	Communication protocols
	Communications characteristics
	External power source
Quality	QA program
	Standards compliance
	Testing
	Equipment qualification
	Dependability
	Safety-grade certification
Functionality	System level function
	Platform functionality

Page intentionally blank